HP LoadRunner

for the Windows operating systems

Software Version: 9.50

Online Monitor Reference

Manufacturing Part Number: T7182-90017

Document Release Date: January 2009

Software Release Date: January 2009

invent

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Table of Contents

PART IV: SYSTEM RESOURCE MONITORING

PART V: NETWORK DELAY MONITORING

PART VI: FIREWALL MONITORING

PART VII: WEB SERVER RESOURCE MONITORING

PART VIII: WEB APPLICATION SERVER MONITORING

PART IX: DATABASE SERVER RESOURCE MONITORING

PART X: STREAMING MEDIA MONITORING

PART XII: APPLICATION COMPONENT MONITORING

PART XIII: APPLICATION DEPLOYMENT MONITORING

PART XIV: MIDDLEWARE PERFORMANCE MONITORING

PART XV: INFRASTRUCTURE RESOURCE MONITORING

PART XVI: APPENDIXES

Welcome to This Guide

Welcome to the *HP LoadRunner Monitor Reference*. This guide describes how to set up the server monitor environment and configure LoadRunner monitors for monitoring data generated during a scenario.

LoadRunner is HP's tool for application performance testing. LoadRunner stresses your entire application to isolate and identify potential client, network, and server bottlenecks.

LoadRunner enables you to test your system under controlled and peak load conditions. To generate load, LoadRunner runs thousands of Virtual Users, or **Vusers**, that are distributed over a network. The Vusers can run on UNIX and Windows-based platforms. Using a minimum of hardware resources, these Vusers provide consistent, repeatable, and measurable load to exercise your application just as real users would. LoadRunner's in–depth reports and graphs provide the information that you need to evaluate the performance of your application.

This chapter includes:

How This Guide Is Organized

This guide contains the following parts:

Part I **Introduction to Online Monitoring**

Introduces you to monitoring scenario execution using the LoadRunner online monitors.

Part II **Web Resource Monitoring**

Describes the Web resource monitoring.

Part III **Transaction Monitoring**

Describes run-time and transaction monitoring.

Part IV **System Resource Monitoring**

Describes system resource monitoring, including the following resource monitors: Windows, UNIX, Server, SNMP, Antara FlameThrower, and SiteScope.

Part V **Network Delay Monitoring**

Describes how to use network monitoring to determine whether your network is causing a delay in the scenario.

Part VI **Firewall Monitoring**

Describes how to use the Firewall server online monitor to measure the performance of a Firewall server during scenario execution.

Part VII **Web Server Resource Monitoring**

Describes Web server resource monitoring, including the following monitors: Apache, iPlanet/Netscape, iPlanet (SNMP), Microsoft IIS.

Part VIII Web Application Server Monitoring

Describes Web application server monitoring, including the following monitors: Ariba, ATG Dynamo, BroadVision, ColdFusion, Fujitsu INTERSTAGE, iPlanet (NAS), Microsoft ASP, Oracle9iAS HTTP, SilverStream, WebLogic (SNMP), WebLogic (JMX), and WebSphere Application Server.

Part IX Database Server Resource Monitoring

Describes database server resource monitoring: DB2, Oracle, SQL server, and Sybase.

Part X Streaming Media Monitoring

Describes streaming media monitoring, including the following monitors: Windows Media Server, RealPlayer audio and video servers, and RealPlayer and Media Clients.

Part XI ERP/CRM Server Resource Monitoring

Describes ERP/CRM server resource monitoring, including the following monitors: SAP Portal, SAP CCMS, SAPGUI, Siebel Server Manager, Siebel Web Server, and PeopleSoft (Tuxedo) server.

Part XII Application Component Monitoring

Describes application component monitoring, using the Microsoft COM+ monitor.

Part XIII Application Deployment Monitoring

Describes application deployment monitoring, using the Citrix MetaFrame server monitor.

Part XIV Middleware Performance Monitoring

Describes middleware performance monitoring, including the following monitors: Tuxedo, and IBM WebSphere MQ server.

Part XV Infrastructure Resource Monitoring

Describes infrastructure resource monitoring, using the Network Client monitor.

Part XVI Appendixes

Contains additional information about using LoadRunner online monitors.

Note: For information about J2EE and .NET Diagnostics monitors, see the *HP Diagnostics User Guide*.

Who Should Read This Guide

This guide is for the following users of LoadRunner:

- Performance Engineers
- Project Manager

This document assumes that you are moderately knowledgeable about enterprise application development and highly skilled in enterprise system and database administration.

LoadRunner Online Documentation

LoadRunner includes a complete set of documentation describing how to use the product. The documentation is available from the help menu and in PDF format. PDFs can be read and printed using Adobe Reader, which can be downloaded from the Adobe Web site (http://www.adobe.com). Printed documentation is also available on demand.

Accessing the Documentation

You can access the documentation as follows:

- From the **Start** menu, click **Start** > **LoadRunner** > **Documentation** and select the relevant document.
- From the **Help** menu, click **Documentation Library** to open the merged help.

Getting Started Documentation

- **Readme.** Provides last-minute news and information about LoadRunner. You access the Readme from the **Start** menu.
- **HP LoadRunner Quick Start** provides a short, step-by-step overview and introduction to using LoadRunner. To access the Quick Start from the Start menu, click **Start** > **LoadRunner** > **Quick Start.**
- **HP LoadRunner Tutorial.** Self-paced printable guide, designed to lead you through the process of load testing and familiarize you with the LoadRunner testing environment. To access the tutorial from the Start menu, click **Start** > **LoadRunner** > **Tutorial.**

LoadRunner Guides

- **HP Virtual User Generator User Guide.** Describes how to create scripts using VuGen. The printed version consists of two volumes, Volume I - *Using VuGen* and Volume II - *Protocols*, while the online version is a single volume. When necessary, supplement this user guide with the online *HP LoadRunner Online Function Reference*.
- **HP LoadRunner Controller User Guide.** Describes how to create and run LoadRunner scenarios using the LoadRunner Controller in a Windows environment.
- **HP LoadRunner Monitor Reference.** Describes how to set up the server monitor environment and configure LoadRunner monitors for monitoring data generated during a scenario.
- **HP LoadRunner Analysis User Guide.** Describes how to use the LoadRunner Analysis graphs and reports after running a scenario to analyze system performance.
- **HP LoadRunner Installation Guide.** Explains how to install LoadRunner and additional LoadRunner components, including LoadRunner samples.

LoadRunner References

- **LoadRunner Function Reference.** Gives you online access to all of LoadRunner's functions that you can use when creating Vuser scripts, including examples of how to use the functions.
- **Analysis API Reference.** This Analysis API set can be used for unattended creating of an Analysis session or for custom extraction of data from the results of a test run under the Controller. You can access this reference from the Analysis Help menu.
- **LoadRunner Controller Automation COM and Monitor Automation Reference.** An interface with which you can write programs to run the LoadRunner Controller and perform most of the actions available in the Controller user interface. You access this reference (**automation.chm)** from the <**LoadRunner Installation**>**/bin** directory.
- **Error Codes and Troubleshooting.** Provides clear explanations and troubleshooting tips for Controller connectivity and Web protocol errors. It also provides general troubleshooting tips for Winsock, SAPGUI, and Citrix protocols.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:
http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Part I

Introduction to Online Monitoring

1

Introduction

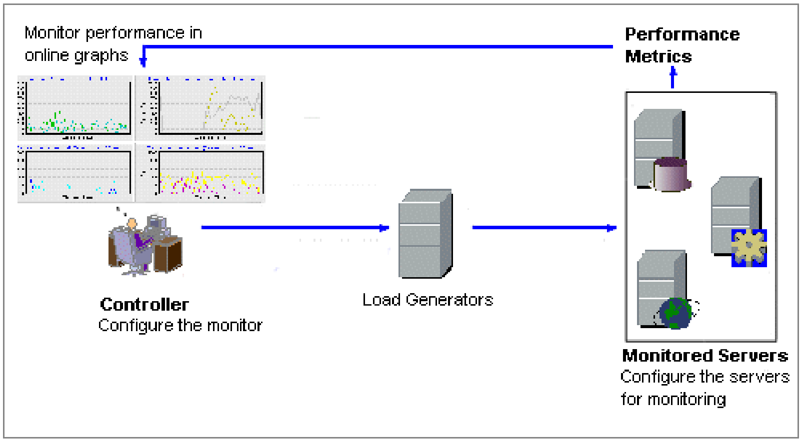
You can monitor a scenario execution using the LoadRunner online monitors.

This chapter includes:

Note: For information on setting monitor options, configuring graph settings and measurements, and exporting graph data, refer to the *HP LoadRunner Controller User Guide*.

Setting Up the Monitoring Environment

Before monitoring a scenario, you need to set up and configure the LoadRunner monitoring components. Each monitor has different configuration requirements that are explained in the specific monitoring chapters. The diagram below illustrates the LoadRunner monitoring process.



Before monitoring a server, perform the following steps:

- ➤ Configure the monitoring environment on the server machine (if necessary)
- ➤ Configure the monitor on the Controller machine

Configuring the Monitoring Environment on the Server Machine

To use the following monitors, you must first install or configure monitoring components on the server machine:

- COM+
- Citrix
- DB2
- IBM WebSphere MQ
- iPlanet (NAS)
- J2EE & .NET Diagnostics
- Network Delay
- Oracle
- PeopleSoft (Tuxedo)
- SAPGUI
- SAP Portal
- SAP CCMS
- Siebel Server Manager
- Siebel Web Server
- SiteScope
- Tuxedo
- UNIX
- WebLogic (JMX)
- WebSphere Application Server

Configuring LoadRunner Monitors on the Controller

To obtain performance data for a monitor, you need to configure the monitor from the Controller, and indicate which statistics and measurements you want to monitor. You select these counters using the monitor's Add Measurements dialog box.

To set up a monitor, you need to perform the following:

- Add a monitored server to the Controller by selecting the server whose monitors you want to configure.
- For SiteScope monitors, configure the remote server.
- Configure the monitor by selecting the measurements that you want to monitor.

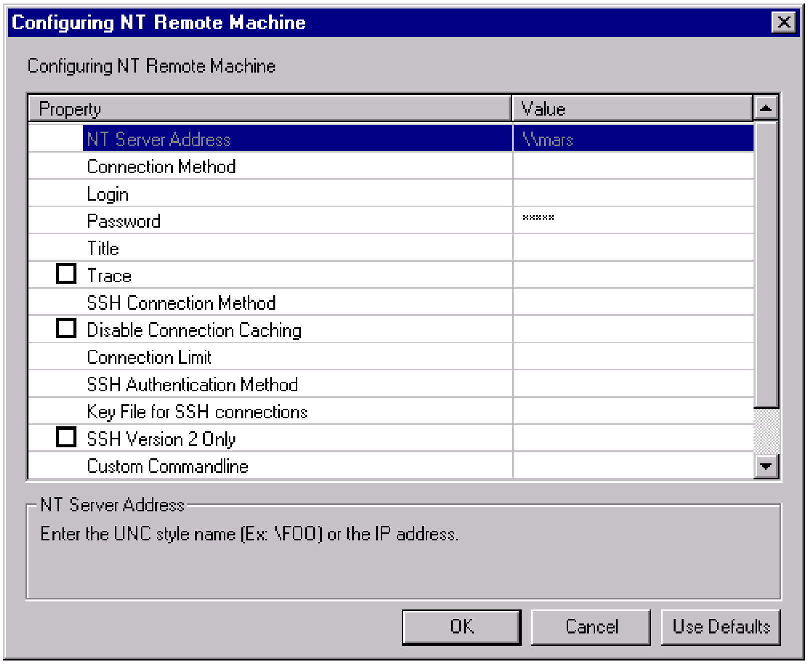
For more information on setting up the monitoring environment and configuring a monitor, see the specific monitoring chapter.

Configuring the Remote Machine for SiteScope Monitors

You configure the remote machine according to your machine's platform: Windows or Unix.

Configuring the Windows Remote Machine

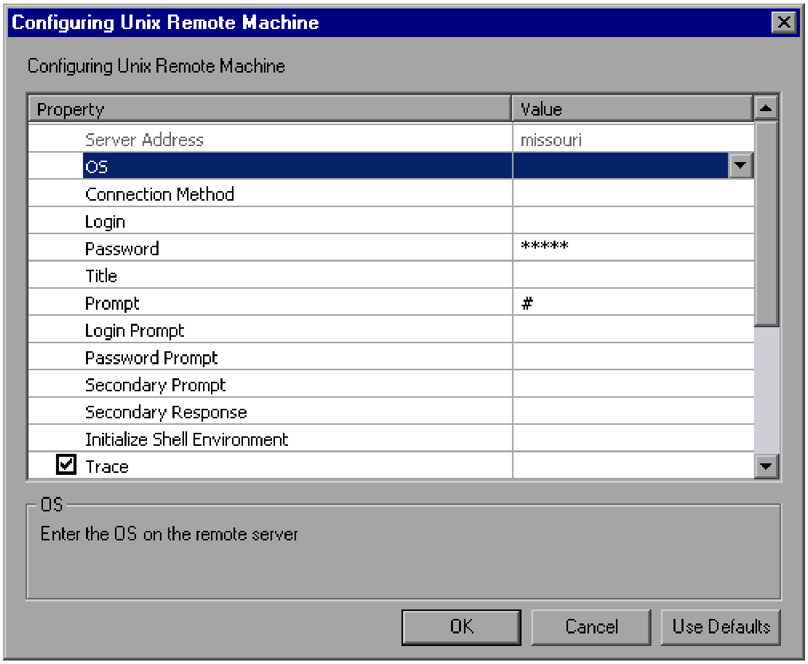
For machines on a Windows platform, when you add measurements to monitor for the first time, the Configuring NT Remote Machine dialog box opens.



Select settings for the remote machine as described in “Understanding the Configuring NT Remote Machine Dialog Box” on page 27.

Configuring the UNIX Remote Machine

For machine on a UNIX platform, when you add measurements to monitor for the first time, the Configuring Unix Remote Machine dialog box opens.



Select settings for the remote machine as described in "Understanding the Configuring Unix Remote Machine Dialog Box" on page 30.

Understanding the Configuring NT Remote Machine Dialog Box

You configure the remote Windows machine from the Configuring NT Remote Machine dialog box.

➤ **NT Server Address.** The IP address or UNC style name of the Windows server you wish to monitor. An IP hostname will also work provided that the SiteScope server has a way to resolve this common name into an IP address (for example, by the use of a hosts file, DNS, or WINS/DNS integration).

- **Connection Method.** SiteScope can use one of two connection types for monitoring remote Windows server resources. These are:
  - **NetBIOS.** The default server-to-server communication protocol for Windows networks.
  - **SSH.** Secure Shell, a more secure communication protocol that can be installed on Windows based networks. This connection method normally requires installing SSH libraries on each server to which you want to connect.
- **Login.** The login for the remote server. If the server is within the same domain as the SiteScope machine, include the domain name in front of the user login name. For example: domainname\user. If you are using a local machine login account for machines within or outside the domain, include the machine name in front of the user login name. For example: machinename\user.
- **Password.** The password for the remote server or the passphrase for the SSH key file.

Note: When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.

- **Title.** (Optional) A name by which the remote machine should be known. This name will appear in the drop-down list.
- **Trace.** Check this box to have trace messages to and from the subject server recorded to the SiteScope RunMonitor.log file.
- **SSH Connection Method.** The method to use for this connection. The currently supported methods are:
  - **Internal Java Libraries.** Connect using the Java SSH client integrated with SiteScope.
  - **Plink.** Connect using an external SSH client. On Windows, SiteScope ships with Plink. On UNIX or Linux SiteScope will use an installed client such as OpenSSH.

- **Disable Connection Caching.** Check this option to turn off connection caching for this remote. By default SiteScope caches open connections.
- **Connection Limit.** Controls the number of open connections that SiteScope will allow for this remote. If you have a large number of monitors configured to use this connection then set this number high enough to relieve the potential bottleneck.

Note: This setting does not effect the running of tests for a remote, tests will always create a new connection.

- **SSH Authentication Method.** The authentication method to use for SSH connections. The currently supported methods are:
  - **Password.** Authenticate using a password.
  - **Key File**. Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file **SiteScope/groups/identity** to authenticate. The corresponding public key must be listed in the **authorized_keys** file on the remote host.
- **Key File for SSH connections.** Select the file that contains the private key for this connection. The default key file is **SiteScope\groups\identity**. This setting only applies when the authentication method is **Key File** .
- **SSH Version 2 Only.** Check this option to force SiteScope to use SSH protocol version 2 only. This option only applies when using the integrated Java Client in SiteScope.
- **Custom Commandline.** Enter a custom commandline for a remote using the External Client. This option can be used when needing to pass specific options to the external client being executed. Valid substitution variable are:
  - $root$. This will be translated to the SiteScope directory.
  - $user$. This will be translated to the username entered into the remote.
  - $password$. This will be translated to the password entered into the remote.
  - $host$. This will be translated to the hostname entered into the remote.

- **SSH Port Number.** Enter the port that the remote SSH server is listening on. By default, the port number is 22.

Understanding the Configuring Unix Remote Machine Dialog Box

You configure the Unix remote machine from the Configuring Unix Remote Machine dialog box.

- **Server Address.** Displays the IP address or host name of the server that you entered in the Add Machine dialog box.
- **OS.** Select the operating system running on the remote server. The following versions of UNIX are supported:

AIX	OPENSERVER
FreeBSD	SCO
HP/UX	SGI Irix
HP/UX 64-bit	Sun Solaris
Linux	Tru64 5.x
MacOSX	Tru64 Pre 4.x (Digital)

- **Connection Method.** Select the method for connecting to the server. The supported methods are:
  - **Telnet.** Log in to the remote server using Telnet.
  - **SSH.** Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX you are working with.
  - **Rlogin.** Log in to the remote server using the Rlogin protocol.
  - **HTTP.** Connect to an HTTP server on the remote server and run the command via a CGI. For this method, the Login and Password are optional and are used for authorizing the log on to the remote machine if required.
- **Login**. The login for the remote server.
- **Password.** Enter the password for the remote server.

- **Title.** Enter a name by which the remote machine should be known. This name will appear in the drop-down list in monitors that can connect to this server.
- **Prompt.** Enter the prompt to be displayed when the system is ready to handle a command - the default is #.
- **Login Prompt.** Enter the prompt to be displayed when the system is waiting for the login to be entered - the default is "login:"
- **Password Prompt.** Enter the prompt to be displayed when the system is waiting for the password to be entered - the default is "password:"
- **Secondary Prompt.** Enter the prompt to be displayed if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt strings by commas (,). For example, for Telnet connections to some remote servers, the remote server may ask what terminal type should be emulated for the connection. In this case you might need to enter Terminal type? as the secondary prompt. The response to the secondary prompt is entered in the Secondary Response field below.
- **Secondary Response.** Enter the responses to secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).
- **Initialize Shell Environment.** Enter any shell commands to be executed at the beginning of the session. Separate multiple commands with a semicolon (;). This option allows you to specify shell commands to be executed on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote.

Examples:

- The remote shell may not have the correct path set for SiteScope scripts to run. The following command will add the directory **/usr/local/bin** into the PATH of the current shell on the remote machine:

  export PATH=$PATH:/usr/local/sbin

- The remote shell may not be initializing the pseudo terminal correctly. Enter the following command to increase the terminal width to 1024 characters:

  stty cols 1024;${SHELL}

Note: Commands after a shell invocation will not be executed.

- There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior.

  Enter the following command to force the remote terminal to echo:

  stty echo

- Certain UNIX shells have been known to behave erratically with SiteScope. This includes bash, ksh, and csh. Enter the following command to change the shell to sh for the SiteScope connection:

  /bin/sh

- **Trace.** Select this option to trace messages to and from the remote server in the **RunMonitor.log** file.
- **SSH Connection Method.** Select the method to use to connect to the remote server.
  - **Internal Java Libraries.** Connect using the Java SSH client integrated with SiteScope
  - **Plink.** Connect using an external SSH client. On Windows, SiteScope ships with Plink.
- **Disable Connection Caching.** Select this to disable SSH connection caching.

- **Connection Limit.** Enter the maximum number of connections for this remote machine.
- **SSH Authentication Method.** Select the method to use to authenticate to the remote server (for SSH connections only).
  - **Password.** Authenticate using a password.
  - **Keyfile.** Authenticate using public/private key authentication. When this option is selected, SiteScope uses the private key in the file **SiteScope/groups/identity** to authenticate. The corresponding public key must be listed in the **authorized_keys** file on the remote host.
- **Connection Limit.** Enter the maximum number of connections for this remote machine.
- **SSH Version 2 Only.** Select this option to force SSH to only use SSH protocol version 2. This option is only supported when using the internal Java libraries connection method.
- **Custom Commandline.** Enter the command for execution of the external SSH client. For substitutions with options listed above, use $host$, $user$, and $password$ respectively. This setting is supported only for connections using an external process.
- **SSH Port Number**. Enter the port on which the SSH service is running.

  After defining the server for SiteScope, you can test the settings by clicking on the test link. SiteScope attempts to display the working directory of the remote machine (the "pwd" command on UNIX, or "cd" on Windows), as a test to ensure that the remote machine can be accessed and can run commands properly.

Choosing Monitors and Measurements on the Controller

You specify the machines and measurements that the Controller will monitor during a scenario execution via the Controller's Run tab. During scenario execution, the collected measurement data will appear in the online graphs.

To select measurements to monitor:

1. Click the graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The monitored server machine dialog box opens.
3. Some monitors are native LoadRunner monitors (by default), but you can also monitor through the SiteScope monitor engine.

   If you want to monitor a server through the SiteScope monitor engine, click **Advanced**.

   In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK**.

   For more information, see the relevant monitoring section.
4. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

   ➤ Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

   ➤ For Sitescope monitors enter the name and port number of the SiteScope server, and specify whether you are using a Secure HTTP connection. To use an account, fill in the relevant account information. For more information, see "Understanding the Add Machine Dialog Box" on page 35.
5. In the **Resource Measurements** section of the monitor dialog box, click **Add**. The Monitor Configuration dialog box opens. Choose the measurements for the specific server, and click **OK** to save your configuration.

Understanding the Add Machine Dialog Box

Adds the machine that you want to monitor to the Monitored Server Machines list.

- **Monitored Machine Information**
  - **Name.** Enter the name or IP address of the machine that you want to monitor.
  - **Platform.** Enter the platform of the machine you want to monitor.

- **SiteScope Server Information.** For monitors that use SiteScope, enter the following SiteScope server information:
  - **Name.** Enter the name of the SiteScope server.
  - **Port.** Enter the SiteScope port (default:8888).
  - **Use Secure HTTP.** Select this to use a Secure HTTP connection.
  - **Use Account.** Select this option to use a specific SiteScope user account. Enter the following account details:
    - **Account.** The SiteScope account name or number
    - **Username.** The username defined to log in to the SiteScope account
    - **Password.** The password defined to log in to the SiteScope account

Monitor Types

The online monitors are divided into the following categories:

- **Web Resource Monitors.** Provide information about the number of Web connections, throughput volume, HTTP responses, server retries, and downloaded pages at the Web servers during the scenario. For more information, see Part II, “Web Resource Monitoring.”
- **Transaction and Run-Time Monitors.** Display the transaction rate and response times, and the number and status of Vusers participating in the scenario, as well as the number and types of errors that the Vusers generate. For more information, see Part III, “Transaction Monitoring.”

- **System Resource Monitors.** Measure the Windows, UNIX, Server, SNMP, Antara FlameThrower, and SiteScope resources used during a scenario. For more information, see Part IV, "System Resource Monitoring."
- **Network Delay Monitor.** Displays information about the network delays on your system. For more information, see Part V, "Network Delay Monitoring."
- **Firewall Monitor.** Measures statistics related to the firewall servers during the scenario. For more information, see Part VI, "Firewall Monitoring."
- **Web Server Resource Monitors.** Measure statistics related to the Apache, Microsoft IIS, iPlanet (SNMP) and iPlanet/Netscape Web servers during the scenario. For more information, see Part VII, "Web Server Resource Monitoring."
- **Web Application Server Resource Monitors.** Measure statistics related to the Ariba, ATG Dynamo, BroadVision, ColdFusion, Fujitsu INTERSTAGE, iPlanet (NAS), Microsoft ASP, Oracle9iAS HTTP, SilverStream, WebLogic (SNMP), WebLogic (JMX), and WebSphere application servers during the scenario. For more information, see Part VIII, "Web Application Server Monitoring."
- **Database Server Resource Monitors.** Measure statistics related to the SQL server, Oracle, Sybase, and DB2 databases during the scenario. For more information, see Part IX, "Database Server Resource Monitoring."
- **Streaming Media Monitors.** Measure statistics related to the Windows Media Server and RealPlayer audio/video servers, as well as the RealPlayer client during the scenario. For more information, see Part X, "Streaming Media Monitoring."
- **ERP/CRM Server Resource Monitors.** Measure statistics related to the SAP Portal, SAP CCMS, SAPGUI, Siebel Server Manager, Siebel Web Server, and PeopleSoft (Tuxedo) servers during the scenario. For more information, see Part XI, "ERP/CRM Server Resource Monitoring."
- **J2EE & .NET Diagnostics Monitors.** Provide information to trace, time, and troubleshoot individual transactions through J2EE Web, application, and database servers. For more information, see the *HP Diagnostics User Guide*.
- **Application Component Monitor.** Measures statistics related to the Microsoft COM+ server during a scenario run. For more information, see Part XII, "Application Component Monitoring."

- **Application Deployment Solutions Monitor.** Measures statistics related to the Citrix MetaFrame XP server during a scenario run. For more information, see Part XIII, "Application Deployment Monitoring."
- **Middleware Performance Monitors.** Measure statistics related to the Tuxedo and IBM WebSphere MQ servers during a scenario run. For more information, see Part XIV, "Middleware Performance Monitoring."
- **Infrastructure Resources Monitor.** Displays information about network client data points during a scenario using the Network Client graph. For more information, see Part XV, "Infrastructure Resource Monitoring."
- **Security Monitor.** Displays information about simulated attacks on the server during a scenario using the Distributed Denial of Service graph. For more information, see Part XVI, "Appendixes."

All of the monitors allow you to view a summary of the collected data at the conclusion of the scenario. Using LoadRunner Analysis, you can generate a graph for any of the monitors. For more information, see the *HP LoadRunner Analysis User Guide*.

Part II

Web Resource Monitoring

2

Web Resource Monitors

You obtain information about the performance of your Web server using LoadRunner's Web Resource monitor.

This chapter includes:

About Web Resource Monitoring

The Web Resource monitor enables you to analyze the throughput on the Web server, the number of hits per second that occurred during the scenario, the number of HTTP responses per second, the HTTP status codes (which indicate the status of HTTP requests, for example, **the request was successful**, **the page was not found**) returned from the Web server, the number of downloaded pages per second, the number of server retries per second, the number of open TCP/IP connections, the number of new TCP/IP connections per second, and the number of SSL Connections per second.

Hits per Second Graph

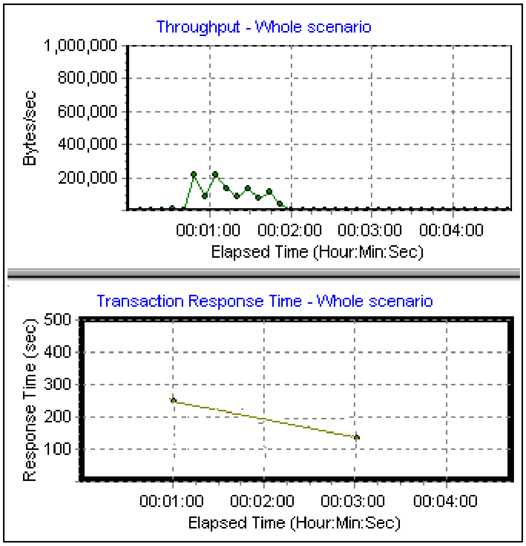
The **Hits Per Second** graph shows the number of hits (HTTP requests) to the Web server (y-axis) as a function of the elapsed time in the scenario (x-axis). This graph can display the whole step, or the last 60, 180, 600, or 3600 seconds. You can compare this graph to the Transaction Response Time graph to see how the number of hits affects transaction performance.

Throughput Graph

The **Throughput** graph shows the amount of throughput on the Web server (y-axis) during each second of the scenario run (x-axis). Throughput is measured in bytes and represents the amount of data that the Vusers received from the server at any given second. You can compare this graph to the Transaction Response Time graph to see how the throughput affects transaction performance.

In the following example, the Transaction Response time graph is compared with the Throughput graph. It is apparent from the graph that as the throughput decreases, the transaction response time also decreases. The peak throughput occurred at approximately 1 minute into the step. The highest response time also occurred at this time.

Example:



HTTP Responses per Second Graph

The **HTTP Responses per Second** graph shows the number of HTTP status codes (y-axis)—which indicate the status of HTTP requests, for example, “the request was successful” or “the page was not found”—returned from the Web server during each second of the scenario run (x-axis), grouped by status code. You can group the results shown in this graph by script (using the "Group By" function) to locate scripts which generated error codes.

The following table displays a list of HTTP status codes:

Code	Description
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content

Code	Description
205	Reset Content
206	Partial Content
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy
307	Temporary Redirect
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Request Entity Too Large
414	Request - URI Too Large
415	Unsupported Media Type

Code	Description
416	Requested range not satisfiable
417	Expectation Failed
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version not supported

For more information on the above status codes and their descriptions, see http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.

Pages Downloaded per Second Graph

The **Pages Downloaded per Second** graph shows the number of Web pages (y-axis) downloaded from the server during each second of the scenario run (x-axis). This graph helps you evaluate the amount of load Vusers generate, in terms of the number of pages downloaded.

Note: To view the Pages Downloaded per Second graph, you must select **Pages per second (HTML Mode only)** from the script's run-time settings Preferences tab before running your scenario.

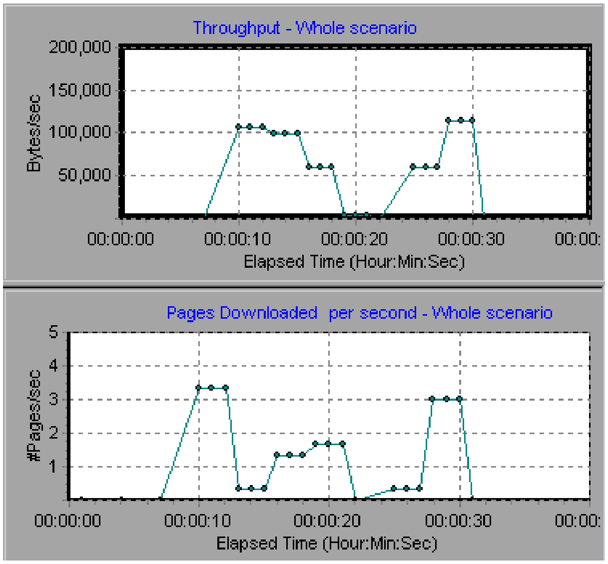
Like throughput, downloaded pages per second is a representation of the amount of data that the Vusers received from the server at any given second.

➤ The Throughput graph takes into account each resource and its size (for example, the size of each **.gif** file, the size of each Web page).

➤ The Pages Downloaded per Second graph takes into account simply the number of pages.

In the following example, the Throughput graph is compared with the Pages Downloaded per Second graph. It is apparent from the graph that throughput is not proportional to the number of pages downloaded per second. For example, between 15 and 16 seconds into the scenario, the throughput decreased while the number of pages downloaded per second increased.

Example:



Retries per Second Graph

The **Retries Per Second** graph shows the number of attempted Web server connections (y-axis) as a function of the elapsed time in the scenario (x-axis). A server connection is retried when the initial connection was unauthorized, when proxy authentication is required, when the initial connection was closed by the server, when the initial connection to the server could not be made, or when the server was initially unable to resolve the load generator's IP address.

Connections Graph

The **Connections** graph shows the number of open TCP/IP connections (y-axis) at each point in time of the scenario (x-axis). One HTML page may cause the browser to open several connections, when links on the page go to different Web addresses. Two connections are opened for each Web server.

This graph is useful in indicating when additional connections are needed. For example, if the number of connections reaches a plateau, and the transaction response time increases sharply, adding connections would probably cause a dramatic improvement in performance (reduction in the transaction response time).

Connections per Second Graph

The **Connections Per Second** graph shows the number of new TCP/IP connections (y-axis) opened and the number of connections that are shut down each second of the scenario (x-axis).

This number should be a small fraction of the number of hits per second, because new TCP/IP connections are very expensive in terms of server, router and network resource consumption. Ideally, many HTTP requests should use the same connection, instead of opening a new connection for each request.

SSLs per Second Graph

The SSLs per Second graph shows the number of new and reused SSL Connections (y-axis) opened in each second of the scenario (x-axis). An SSL connection is opened by the browser after a TCP/IP connection has been opened to a secure server.

Because creating a new SSL connection entails heavy resource consumption, you should try to open as few new SSL connections as possible; once you've established an SSL connection, you should reuse it. There should be no more than one new SSL connection per Vuser.

If you set your run-time settings to simulate a new Vuser at each iteration (via the Browser Emulation tab in the Run-Time Settings menu), you should have no more than one new SSL connection per Vuser per iteration. Ideally, you should have very few new TCP/IP and SSL connections each second.

Part III

Transaction Monitoring

3

Run-Time and Transaction Monitoring

While running a scenario, you use LoadRunner's Run-Time and Transaction monitors to view graphs of run-time status and transaction performance.

This chapter includes:

About Run-Time and Transaction Graphs

The **Run-Time** monitor provides information about the status of the Vusers participating in the scenario, and the number and types of errors that the Vusers generate. In addition, the Run-Time monitor provides the User-Defined Data Points graph, which displays the real time values for user-defined points in a Vuser script.

The **Transaction** monitor displays the transaction rate and response time during scenario execution. For more information about transactions, see "Adding Transactions to a Script" on page 56.

Run-Time Graphs

The **Runtime** monitor provides information for the following graphs:

➤ Running Vusers Graph

➤ User-Defined Data Points Graph

➤ Error Statistics Graph

➤ Vusers with Errors Graph

Running Vusers Graph

The monitor's **Running Vusers** graph provides information about the status of the Vusers running in the current scenario on all load generator machines. The graph shows the number of running Vusers, while the information in the legend indicates the number of Vusers in each state.

Color	Scale	Status	Max	Min	Avg	Std	Last
	1	Running	14	2	7.632653...	3.783389...	14
	1	Error	0	0	0	0	0
	1	Finished	0	0	0	0	0

The Status field of each Vuser displays the current status of the Vuser. The following table describes each Vuser status.

Status	Description
Running	The total number of Vusers currently running on all load generators.
Ready	The number of Vusers that completed the initialization section of the script and are ready to run.
Finished	The number of Vusers that have finished running. This includes both Vusers that passed and failed.
Error	The number of Vusers whose execution generated an error. Check the Status field in the Vuser view or the Output window for a complete explanation of the error.

User-Defined Data Points Graph

The **User-Defined Data Points** graph displays the real-time values of user-defined data points. You define a data point in your Vuser script by inserting an **lr_user_data_point** function at the appropriate place (**user_data_point** for GUI Vusers and **lr.user_data_point** for Java Vusers).

```
Action1()
{
 lr_think_time(1);
 lr_user_data_point ("data_point_1",1);
 lr_user_data_point ("data_point_2",2);
 return 0;
}
```

For Vuser protocols that support the graphical script representations such as Web and Oracle NCA, you insert a data point as a user-defined step. Data point information is gathered each time the script executes the function or step. For more information about data points, see the *HP LoadRunner Online Function Reference*.

By default, LoadRunner displays all of the data points in a single graph. The legend provides information about each data point. If desired, you can hide specific data points using the legend below the graphs.

You can also view data points offline, after the completion of the scenario. For more information, see the *HP LoadRunner Analysis User Guide*.

Error Statistics Graph

The monitor's **Error Statistics** graph provides details about the number of errors that accrue during each second of the scenario run. The errors are grouped by error source—for example, the location in the script or the load generator name.

Vusers with Errors Graph

The **Vusers with Errors** graph provides details about the number of Vusers that generate errors during scenario execution. The errors are grouped by error source.

Transaction Monitor Graphs

The **Transaction** monitor provides the following graphs:

- Transaction Response Time
- Transactions per Second (Passed)
- Transactions per Second (Failed, Stopped)
- Total Transactions per Second (Passed)

The **Transaction Response Time** graph shows the average response time of transactions in seconds (y-axis) as a function of the elapsed time in the scenario (x-axis).

The **Transactions per Second (Passed)** graph shows the number of successful transactions performed per second (y-axis) as a function of the elapsed time in the scenario (x-axis).

The **Transactions per Second (Failed, Stopped)** graph shows the number of failed and stopped transactions per second (y-axis) as a function of the elapsed time in the scenario (x-axis).

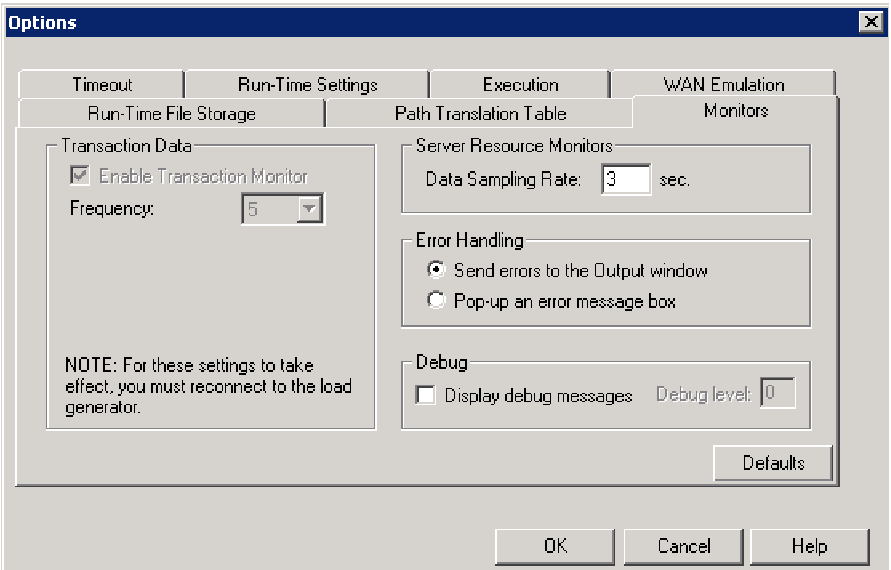
The **Total Transactions per Second (Passed)** graph shows the total number of completed, successful transactions per second (y-axis) as a function of the elapsed time in the scenario (x-axis).

Enabling the Transaction Monitor

The Transaction monitor is enabled by default—it automatically begins monitoring Vuser transactions at the start of a scenario. To conserve resources, you can disable the Transaction monitor.

To disable the Transaction monitor:

1 Choose **Tools** > **Options** and select the **Monitors** tab.



2 Disable transaction monitoring by clearing the **Enable Transaction Monitor** check box. To enable transaction monitoring, select the **Enable Transaction Monitor** check box.

Adding Transactions to a Script

If there are no transactions defined in your Vuser script, no data will be displayed in the online graphs. To add transactions to an existing script, edit it using the appropriate tool. The following table shows the script generation tools for each script type:

Script type	Editing tool
QTP scripts	WinRunner
VuGen scripts	VuGen (Virtual User Generator)

To add a transaction to a script in the Controller:

1 Click the **Design** tab to view the list of Vuser groups and scripts.

2 To edit a script for a Vuser group, select the group and click the **View Script** button to the right of the Scenario Groups window. The script generation tool opens.

To edit a script for an individual Vuser, click **Vusers**. Right-click the Vuser whose script you want to edit, and select **View Script** to open the script generation tool.

3 Insert Start and End Transaction functions or markers throughout your script.

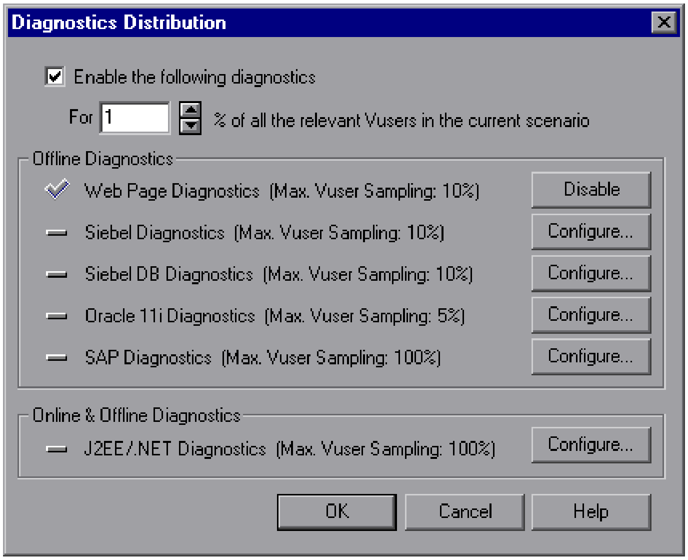
For more information, see the appropriate user's guide as described in the *Welcome* chapter.

Enabling Web Page Diagnostics

In order for the Analysis to generate Web Page Diagnostics graphs, which provide you with performance information for each transaction and sub-transaction defined in your script, you must enable the Web page Diagnostics feature in the Controller before running your scenario.

To enable Web Page Diagnostics in the Controller:

1. From the Controller's Run tab, choose **Diagnostics** > **Configuration**. The Diagnostics Distribution dialog box opens.



2. Select **Enable the following diagnostics** and specify the percentage of Vusers for which you want transaction breakdown to be performed.
3. Click the **Enable** button next to **Web Page Diagnostics (Max. Vuser Sampling: 10%)**.
4. Click **OK**.

For more information, refer to the "Working with Diagnostics" section of the *HP LoadRunner Controller User Guide*.

For more information about Web Page Breakdown graphs, refer to the *HP LoadRunner Analysis User Guide*.

Part IV

System Resource Monitoring

4

Understanding System Resource Monitors

You use LoadRunner's System Resource monitors to monitor a machine's system resource usage during a scenario run and isolate server performance bottlenecks.

A primary factor in a transaction's response time is its system resource usage. Using the LoadRunner resource monitors, you can monitor the Windows, UNIX, Server, SNMP, Antara FlameThrower, and SiteScope resources on a machine during a scenario run, and determine why a bottleneck occurred on a particular machine.

The Windows measurements correspond to the built-in counters available from the Windows Performance Monitor.

The UNIX measurements include those available by the **rstatd** daemon: average load, collision rate, context switch rate, CPU utilization, incoming packets error rate, incoming packets rate, interrupt rate, outgoing packets error rate, outgoing packets rate, page-in rate, page-out rate, paging rate, swap-in rate, swap-out rate, system mode CPU utilization, and user mode CPU utilization.

Note: You must configure an **rstatd** daemon on all UNIX machines being monitored. For information on how to configure an **rstatd** daemon, refer to the UNIX *man* pages, or see "Setting up the Monitoring Environment" on page 79.

The Server Resources monitor can measure CPU, disk space, memory, and application resources used on remote Windows and UNIX servers.

The SNMP monitor is available for monitoring machines using the Simple Network Management Protocol (SNMP). SNMP monitoring is platform independent.

The Antara FlameThrower monitor can measure the following performance counters: Layer, TCP, HTTP, SSL/HTTPS, Sticky SLB, FTP, SMTP, POP3, DNS, and Attacks.

The SiteScope monitor can measure server, network, and processor performance counters. For detailed information on the performance counters that SiteScope can monitor, see the relevant SiteScope documentation.

The resource monitors are automatically enabled when you execute a scenario. However, you must specify the machine you want to monitor and which resources to monitor for each machine. You can also add or remove machines and resources during the scenario run.

For more information about a particular System Resource monitor see:

➤ Chapter 5, "Windows Resource Monitoring"

➤ Chapter 6, "UNIX Resource Monitoring"

➤ Chapter 7, "Server Resource Monitoring"

➤ Chapter 8, "SNMP Resource Monitoring"

➤ Chapter 9, "SiteScope Resource Monitoring"

5

Windows Resource Monitoring

The Windows Resources monitor shows the Windows resources measured during the scenario. Windows measurements correspond to the built-in counters available from the Windows Performance Monitor.

Note: To monitor a Windows machine over a firewall, use TCP, port 139.

This chapter includes:

Setting up the Monitoring Environment

- If you are using the SiteScope monitor engine, ensure that SiteScope has been installed on a server. You can install SiteScope on the same server as the Controller, or on a dedicated server.
- If you want to monitor a remote Windows server that does not use Windows domain security, you must authenticate the Controller on the remote Windows server. To authenticate the Controller, create an account, or change the password of the account used to log on to the Controller so that it matches the password and user name used to log on to the remote monitored Windows machine. When the remote Windows machine requests another machine's resources, it sends the logged-in user name and password of the machine requesting the resources.

Adding a Machine to Monitor

In order to monitor the Windows resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the **Windows Resources** graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Windows Resources dialog box opens.
3. By default, LoadRunner monitors Windows resources using the native LoadRunner monitor engine.

   If you want to monitor Windows resources using the SiteScope monitor engine, click **Advanced**.

   In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK** to close the Monitor Engine dialog box.

4 In the **Monitored Server Machines** section, click **Add**.

The Add Machine dialog box opens.

- In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs.
- In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

  Note: If you are adding a native LoadRunner monitor, the **SiteScope Server Information** section does not appear.

Click **OK** to close the Add Machine dialog box.

5 Click **Add** in the **Resource Measurements on:** <*machine*> section of the Windows Resources dialog box.

6 Continue with "Configuring the Windows Resources Monitor" on page 65.

Configuring the Windows Resources Monitor

The configuration for this monitor differs slightly depending on whether you are adding a native LoadRunner or SiteScope monitor.

This section describes:

- Configuring the Native LoadRunner Windows Resources Monitor
- Configuring the SiteScope Windows Resources Monitor

Configuring the Native LoadRunner Windows Resources Monitor

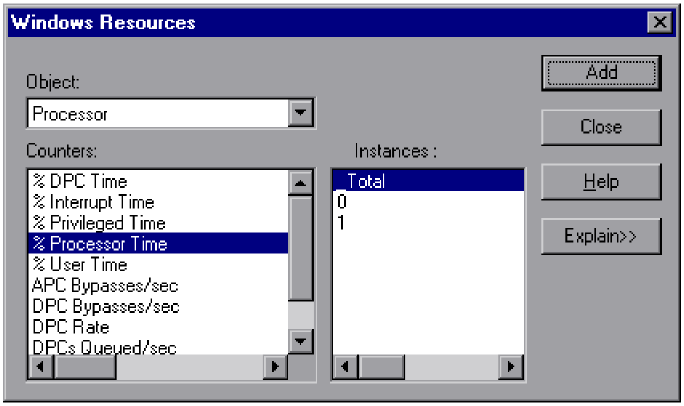
1 When you add a machine in the Windows Resources dialog box, the default measurements are displayed in the **Resource Measurements on:** <*machine*> section.

Note: To change the default counters for the Windows machine monitor, see “Changing a Monitor’s Default Counters” on page 395.

➤ To delete a measurement from the default list, select the measurement and click **Delete**.

➤ To select additional measurements, click **Add**.

2 A Windows Resources dialog box opens displaying the available Windows resources.



For each measurement select an object, counter, and instance, as described in “Understanding the Add Windows Resources Measurements Dialog Box” on page 68, and then click **Add**.

For a description of the available measurements, see “Windows Resource Performance Counters” on page 69.

3 When you have finished selecting the measurements to monitor, click **Close**. The counters that you selected appear in the **Resource Measurements on**: <*machine*> section of the Windows Resources dialog box.

4 Click **OK** in the Windows Resources dialog box to activate the monitor.

Configuring the SiteScope Windows Resources Monitor

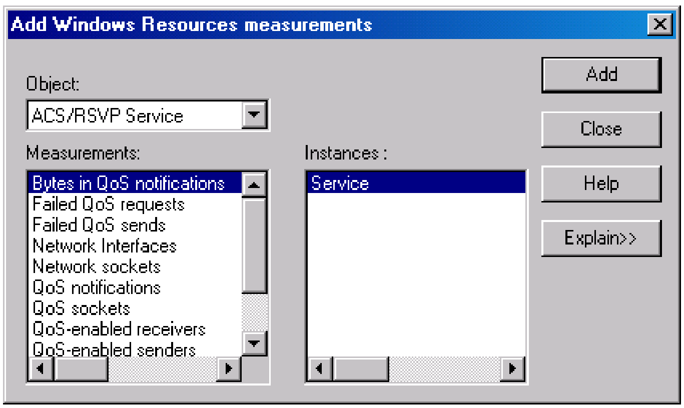
The first time you add measurements you need to configure the remote machine properties. When you click **Add** in the **Resource Measurements on:** <*machine*> section of the Windows Resources dialog box, the Configuring NT Remote Machine dialog box opens.

To configure a SiteScope Windows Resources monitor:

1 Enter the remote machine's configuration information, as described in "Understanding the Configuring NT Remote Machine Dialog Box" on page 27, and click **OK**.

2 The Configuring PDH Monitor dialog box opens. Verify the **Server** and **Update every** properties, and click **OK**.

3 The Add Windows Resources Measurements dialog box opens displaying the available measurements and server properties.



For each measurement select an object, measurement, and instance, as described in "Understanding the Add Windows Resources Measurements Dialog Box" on page 68, and then click **Add**.

For a description of the available measurements, see "Windows Resource Performance Counters" on page 69.

Note: To change the default counters for the Windows machine monitor, see "Changing a Monitor's Default Counters" on page 395.

---

4 When you have finished selecting the measurements to monitor, click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the Windows Resources dialog box.

5 Click **OK** in the Windows Resources dialog box to activate the monitor.

Understanding the Add Windows Resources Measurements Dialog Box

The Add Windows Resources Measurements dialog box lets you select the Windows resources to monitor. The Windows resources correspond to the built-in counters available from the Windows Performance Monitor.

➤ **Object.** Select the object to monitor on the specified Windows machine.

➤ **Counters/Measurements.** Select the resource counter/measurement to monitor. Select multiple counters using the CTRL key. For an explanation of each counter, click **Explain**.

➤ **Instances.** If multiple instances of the selected counter are running, select one or more instances to monitor for the selected counter.

➤ **Explain.** Displays a description of the selected counter.

Windows Resource Performance Counters

The following default measurements are available for Windows machines:

Object	Measurement	Description
System	**% Total Processor Time**	The average percentage of time that all the processors on the system are busy executing non-idle threads. On a multi-processor system, if all processors are always busy, this is 100%, if all processors are 50% busy this is 50% and if 1/4 of the processors are 100% busy this is 25%. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process which consumes those unproductive processor cycles not used by any other threads.
System	**File Data Operations/sec**	The rate at which the computer issues read and write operations to file system devices. This does not include File Control Operations.
Processor	**% Processor Time (Windows 2000)**	The percentage of time that the processor is executing a non-idle thread. This counter was designed as a primary indicator of processor activity. It is calculated by measuring the time that the processor spends executing the thread of the idle process in each sample interval, and subtracting that value from 100%. (Each processor has an idle thread which consumes cycles when no other threads are ready to run). It can be viewed as the percentage of the sample interval spent doing useful work. This counter displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time the service was inactive, and then subtracting that value from 100%.

Object	Measurement	Description
System	**Processor Queue Length**	The instantaneous length of the processor queue in units of threads. This counter is always 0 unless you are also monitoring a thread counter. All processors use a single queue in which threads wait for processor cycles. This length does not include the threads that are currently executing. A sustained processor queue length greater than two generally indicates processor congestion. This is an instantaneous count, not an average over the time interval.
Memory	**Page Faults/sec**	This is a count of the page faults in the processor. A page fault occurs when a process refers to a virtual memory page that is not in its Working Set in the main memory. A page fault will not cause the page to be fetched from disk if that page is on the standby list (and hence already in main memory), or if it is in use by another process with which the page is shared.
PhysicalDisk	**% Disk Time**	The percentage of elapsed time that the selected disk drive is busy servicing read or write requests.
Memory	**Pool Nonpaged Bytes**	The number of bytes in the nonpaged pool, a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Nonpaged pool pages cannot be paged out to the paging file. They remain in main memory as long as they are allocated.

Object	Measurement	Description
Memory	**Pages/sec**	The number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system cache to access file data for applications. This value also includes the pages to/from non-cached mapped memory files. This is the primary counter to observe if you are concerned about excessive memory pressure (that is, thrashing), and the excessive paging that may result.
System	**Total Interrupts/sec**	The rate at which the computer is receiving and servicing hardware interrupts. The devices that can generate interrupts are the system timer, the mouse, data communication lines, network interface cards, and other peripheral devices. This counter provides an indication of how busy these devices are on a computer-wide basis. See also Processor:Interrupts/sec.
Objects	**Threads**	The number of threads in the computer at the time of data collection. Notice that this is an instantaneous count, not an average over the time interval. A thread is the basic executable entity that can execute instructions in a processor.
Process	**Private Bytes**	The current number of bytes that the process has allocated that cannot be shared with other processes.

6

UNIX Resource Monitoring

The UNIX Resources monitor shows the UNIX resources measured during the scenario. This graph helps you determine the impact of Vuser load on the various system resources.

The UNIX kernel statistics measurements include those available by the rstatd daemon: average load, collision rate, context switch rate, CPU utilization, incoming packets error rate, incoming packets rate, interrupt rate, outgoing packets error rate, outgoing packets rate, page-in rate, page-out rate, paging rate, swap-in rate, swap-out rate, system mode CPU utilization, and user mode CPU utilization.

To obtain data for this graph, you need to select the desired measurements for the online monitor (from the Controller) before running the scenario.

This chapter includes:

Setting up the Monitoring Environment

To monitor UNIX resources, you must configure the rstatd daemon.

Note: The rstatd daemon might already be configured, because when a machine receives an rstatd request, the inetd on that machine activates the rstatd automatically.

To verify whether the rstatd daemon is already configured:

The **rup** command reports various machine statistics, including rstatd configuration. Run the following command to view the machine statistics:

```
>rup host
```

You can also use **lr_host_monitor** and see if it returns any relevant statistics.

If the command returns meaningful statistics, the rstatd daemon is already configured and activated. If not, or if you receive an error message, the rstatd daemon is not configured.

To configure the rstatd daemon:

1. Run the command: su root
2. Go to **/etc/inetd.conf** and look for the rstatd row (it begins with the word rstatd). If it is commented out (with a #), remove the comment directive, and save the file.
3. From the command line, run:

   ```
   kill -1 inet_pid
   ```

   where **inet_pid** is the pid of the inetd process. This instructs the inetd to rescan the **/etc/inetd.conf** file and register all daemons which are uncommented, including the rstatd daemon.
4. Run *rup* again.

   If the command still does not indicate that the rstatd daemon is configured, contact your system administrator.

Note: To monitor a UNIX machine through a firewall, you must run a UNIX utility called **rpcinfo** and identify the rstatd's port number. By running rpcinfo -p <hostname>, you will receive a list of all RPC servers registered in the host's portmapper, along with the port number. This list will not change until rstatd is stopped and rerun.

Some firewalls allow you to open an RPC program number instead of a port. In such cases, open program 100001. If are prompted to include a version number, specify versions 3 and 4.

Adding a Machine to Monitor

In order to monitor the UNIX Resources of a particular machine from the Controller, you need to add the machine and the measurements you want to monitor.

To add a machine to the Controller:

1. Click the UNIX Resources graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The UNIX Resources dialog box opens.

   In the **Monitored Server Machines** section, click **Add**. The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor, and click **OK**.
4. In the **Resource Measurements** section of the UNIX Resources dialog box, select the measurements you want to monitor.

   For a description of the available measurements, see "UNIX Resources Performance Counters" on page 78.

Note: To change the default counters for the UNIX monitor, see "Changing a Monitor's Default Counters" on page 395.

5 To select additional measurements, click **Add**.

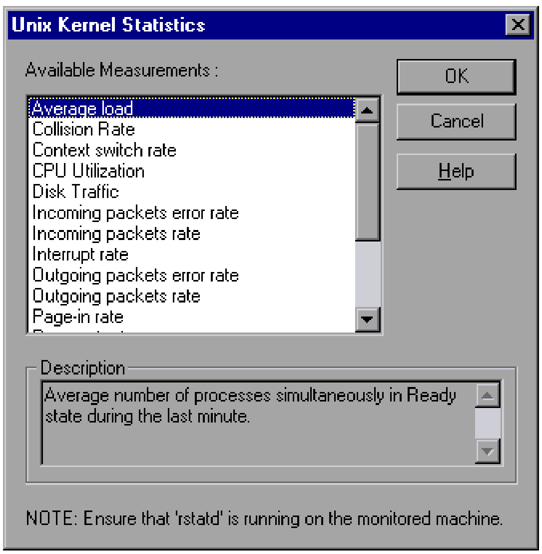
6 Continue with Configuring the UNIX Resources Monitor below.

Configuring the UNIX Resources Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the UNIX Resources monitor:

1 When you click **Add** in the **Resource Measurements on:** <*machine*> section of the UNIX Resources dialog box, the UNIX Kernel Statistics dialog box opens, displaying the available measurements and server properties.



Select measurements and server properties as described in "Understanding the Unix Kernel Statistics Dialog Box" on page 77.

For a description of the available measurements, see "UNIX Resources Performance Counters" on page 78.

2 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the UNIX Resources dialog box.

3 Click **OK** in the UNIX Resources dialog box to activate the monitor.

Note: Ensure that the rstatd daemon is correctly configured and running on the monitored UNIX machine. For more information, see "Setting up the Monitoring Environment" on page 74.

To change the default counters for the UNIX monitor, see "Changing a Monitor's Default Counters" on page 395.

Understanding the Unix Kernel Statistics Dialog Box

The UNIX Kernel Statistics dialog box lets you select the UNIX kernel statistics to monitor.

The UNIX kernel statistics measurements include those available by the rstatd daemon: average load, collision rate, context switch rate, CPU utilization, incoming packets error rate, incoming packets rate, interrupt rate, outgoing packets error rate, outgoing packets rate, page-in rate, page-out rate, paging rate, swap-in rate, swap-out rate, system mode CPU utilization, and user mode CPU utilization.

- **Available Measurements.** Select the measurements you want to add. To select more than one measurement, use the CTRL key.
- **Description.** Displays a description of the selected measurement.

Note: Ensure that rstatd is running on the monitored UNIX machine. For more information, see "Setting up the Monitoring Environment" on page 74.

UNIX Resources Performance Counters

The following default measurements are available for the UNIX machine:

Measurement	Description
Average load	Average number of processes simultaneously in Ready state during the last minute
Collision rate	Collisions per second detected on the Ethernet
Context switches rate	Number of switches between processes or threads, per second
CPU utilization	Percent of time that the CPU is utilized
Disk rate	Rate of disk transfers
Incoming packets error rate	Errors per second while receiving Ethernet packets
Incoming packets rate	Incoming Ethernet packets per second
Interrupt rate	Number of device interrupts per second
Outgoing packets errors rate	Errors per second while sending Ethernet packets
Outgoing packets rate	Outgoing Ethernet packets per second
Page-in rate	Number of pages read to physical memory, per second
Page-out rate	Number of pages written to pagefile(s) and removed from physical memory, per second
Paging rate	Number of pages read to physical memory or written to pagefile(s), per second
Swap-in rate	Number of processes being swapped
Swap-out rate	Number of processes being swapped
System mode CPU utilization	Percent of time that the CPU is utilized in system mode
User mode CPU utilization	Percent of time CPU is utilized in user mode

7

Server Resource Monitoring

The Server Resources monitor shows the resources of monitors (CPU, disk space, memory, or applications) used on remote Windows and UNIX servers measured during the scenario. This helps you determine the impact of Vuser load on the various system resources.

The Server Resources monitor includes the following monitors:

➤ **CPU Monitor.** Monitors CPU usage.

➤ **Disk Space Monitor.** Monitors disk space.

➤ **Memory Monitor.** Monitors Pages per Second and Percentage of Virtual Memory Used.

➤ **Service Monitor.** Verifies that specific processes are listed as running and checks CPU usage.

To obtain data for this graph, you need to select the desired measurements for the online monitor (from the Controller) before running the scenario.

This chapter includes:

Setting up the Monitoring Environment

➤ Ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.

➤ Verify that SiteScope is collecting the required data from the servers it is monitoring. From the SiteScope Panel, select the monitor group polling the Server Resource machines, and check that the monitor displays a list of server measurements in the Status column.

Adding a Machine to Monitor

In order to monitor the server resources of a particular machine from the Controller, you need to add the machine and the measurements you want to monitor.

To add a machine to the Controller:

1. Click the Server Resource graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Server Resources dialog box opens.
3. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
4. In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor, and select the platform on which the machine runs.

Note: If you are using the HTTP method of monitoring, enter the full URL of the CGI script (for example: http://demo.thiscompany.com/cgi-bin/run.sh).

In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

5. Click **OK**. The Server Resources dialog box is redisplayed.

6 In the **Resource Measurements** section of the Server Resources dialog box, click **Add** to configure the remote machine and select the measurements that you want to monitor.

7 Continue with Configuring the Server Resources Monitor below.

Configuring the Server Resources Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

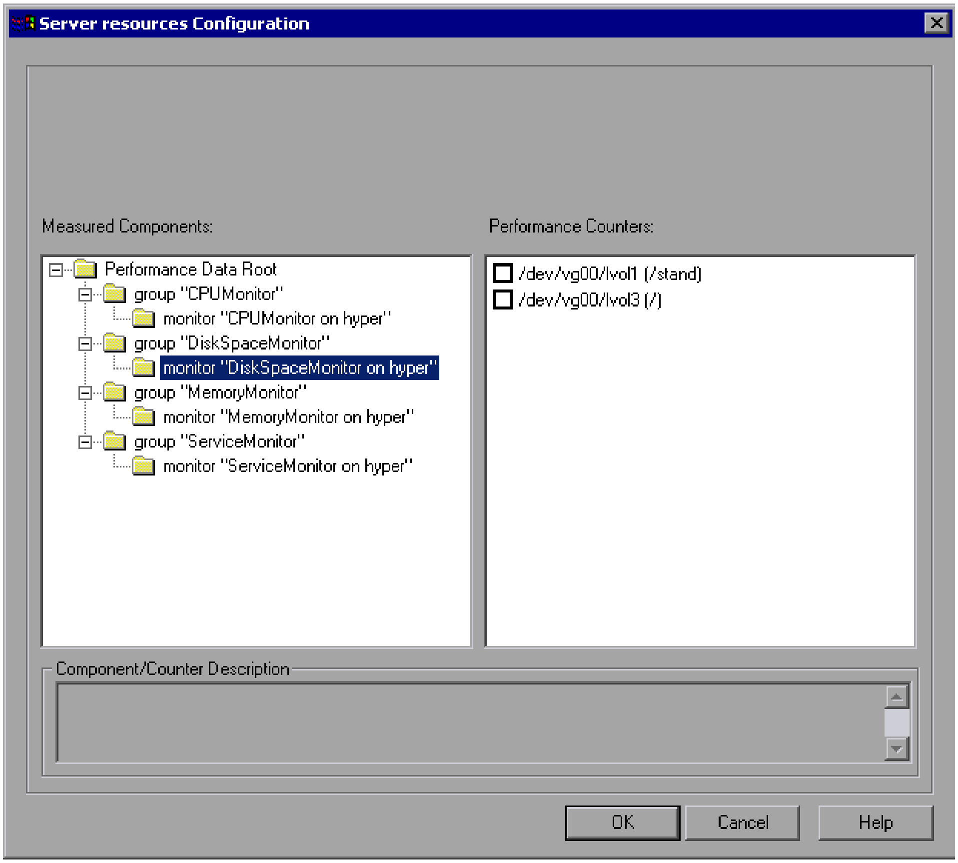
To configure the Server Resources monitor:

1 The first time you add measurements you need to configure the remote machine properties. When you click **Add** in the **Resource Measurements on:** <*machine*> of the Server Resources dialog box, a dialog box opens to configure the remote machine as follows:

- If you are monitoring a machine on a Windows platform, the Configuring NT Remote Machine dialog box opens.
- If you are monitoring a machine on a UNIX platform, the Configuring UNIX Remote Machine dialog box opens.

Enter the remote machine's configuration information, as described in "Configuring the Remote Machine for SiteScope Monitors" on page 25, and click **OK**.

2 The Server Resources Configuration dialog box opens, displaying the available measurements.



Browse the **Measured Components** tree, select the required performance counters in the right pane, as described in "Understanding the Server Resources Configuration Dialog Box" on page 83.

For a list of the available performance counters, see "Server Resources Performance Counters" on page 84.

3 Click **OK.** The components that you selected appear in the **Resource Measurements on**: *<machine>* section of the Server Resources dialog box.

4 In the Controller, click **OK** in the Server Resources dialog box to activate the monitor.

Note: The minimum recommended online graph refresh rate (in the Graph Configuration dialog box) is 30 seconds. If you choose a lower refresh rate, the Controller may not get all the data in time.

Understanding the Server Resources Configuration Dialog Box

The Server Resources Configuration dialog box enables you to select the server resources to monitor.

➤ **Host.** Displays the name of the monitored machine.

➤ **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.

➤ **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.

➤ **Component/Counter Description.** Displays a description of the selected component or counter.

Server Resources Performance Counters

Monitor	Measurements	Description
CPU Monitor	**Utilization**	Measures CPU utilization.
Disk Space Monitor	**Disk space**	Measures the percentage of disk space used.
Memory Monitor	**MB free**	Measures the amount of disk space free, in MB.
	Pages/sec	Measures the number of virtual memory pages that are moved between main memory and disk storage.
	Percent used	Measures the percentage of memory and paging file space used.
Services Monitor		Monitors processes locally or on remote systems. Can be used to verify that specific processes are running.

8

SNMP Resource Monitoring

The SNMP Resources monitor shows statistics for machines using the Simple Network Management Protocol (SNMP). The SNMP Resources monitor is available for monitoring any machine that runs an SNMP agent, using the Simple Network Management Protocol (SNMP).

Note: The LoadRunner SNMP monitor is the same as the SiteScope SNMP by MIB monitor.

This chapter includes:

Setting up the Monitoring Environment

- To obtain data for this graph, you need to configure the SNMP Resources monitor (from the Controller) and select the measurements you want to display, before running the scenario.
- If you are using the SiteScope monitor engine, ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.

Adding a Machine to Monitor

In order to monitor the SNMP Resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the **SNMP Resources** graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The SNMP dialog box opens.
3. By default, LoadRunner monitors SNMP resources using the native LoadRunner monitor engine.

   If you want to monitor SNMP resources using the SiteScope monitor engine, click **Advanced**.

   In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK**.
4. In the **Monitored Server Machines** section, click **Add**.

   The Add Machine dialog box opens.

   ➤ In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs.

   ➤ In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

   Note: If you are adding a native LoadRunner monitor, the **SiteScope Server Information** section does not appear.

   Click **OK** to close the Add Machine dialog box.
5. In the **Resource Measurements on:** <*machine*> section of the SNMP dialog box, click **Add**.
6. Continue with Configuring the SNMP Resources Monitor below.

Configuring the SNMP Resources Monitor

The configuration for this monitor differs slightly depending on whether you are adding a SiteScope or native LoadRunner monitor.

This section describes:

- Configuring the Native LoadRunner SNMP Monitor
- Configuring the SiteScope SNMP by MIB Monitor

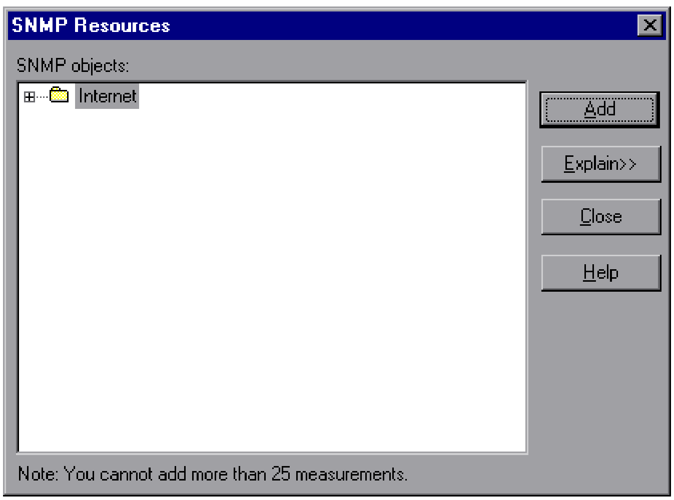
Configuring the Native LoadRunner SNMP Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which objects to monitor on the machine.

To configure the SNMP Resources monitor:

1 When you click **Add** to add a measurement, the SNMP Resources dialog box opens.

Browse the **SNMP Objects** tree, and select and add SNMP resources, as described in “Understanding the SNMP Resources Dialog Box” on page 88.



2 Click **Close**. The resources that you selected appear in the **Resource Measurements on**: <*machine*> section of the SNMP dialog box.

Note: The native LoadRunner SNMP monitor can only monitor up to 25 measurements.

---

3 Click **OK** in the SNMP dialog box to activate the monitor.

Understanding the SNMP Resources Dialog Box

The SNMP Resources dialog box enables you to select the Windows or UNIX resources to monitor using the Simple Network Management Protocol (SNMP).

➤ **SNMP Objects.** Select each required object and click **Add**. Click **Explain** for the ID number and a description of the selected object.

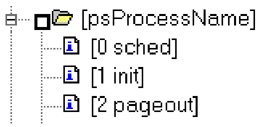
➤ **Explain.** Displays a description of the selected object.

Note: The native LoadRunner SNMP monitor can only monitor up to 25 measurements.

Improving the Level of Measurement Information

You can improve the level of measurement information for the SNMP monitor by enabling measurements with string values to be listed (in addition to measurements with numeric values), and by enabling the name modifier (which displays the string value as an identifying part of the measurement name).

In the following example of a measurement using the name modifier, the string value of ProcessName (sched) is displayed in addition to its instance ID (0):



To enable this feature, add the following line to the <**LoadRunner root folder**>**\dat\monitors\snmp.cfg** file:

```
SNMP_show_string_nodes=1
```

Usage Notes: You can select more than one name modifier, but the first in the hierarchy will be used. Each time the SNMP Add Measurements dialog box opens, the information is reread from the **snmp.cfg** file. You cannot add the same measurement twice (once with a name modifier and once without it). If you do so, an error message is issued.

Note: You can modify the list of resources that you want to monitor at any point during the scenario. A scenario does not have to be active in order for you to monitor the resources on a remote machine.

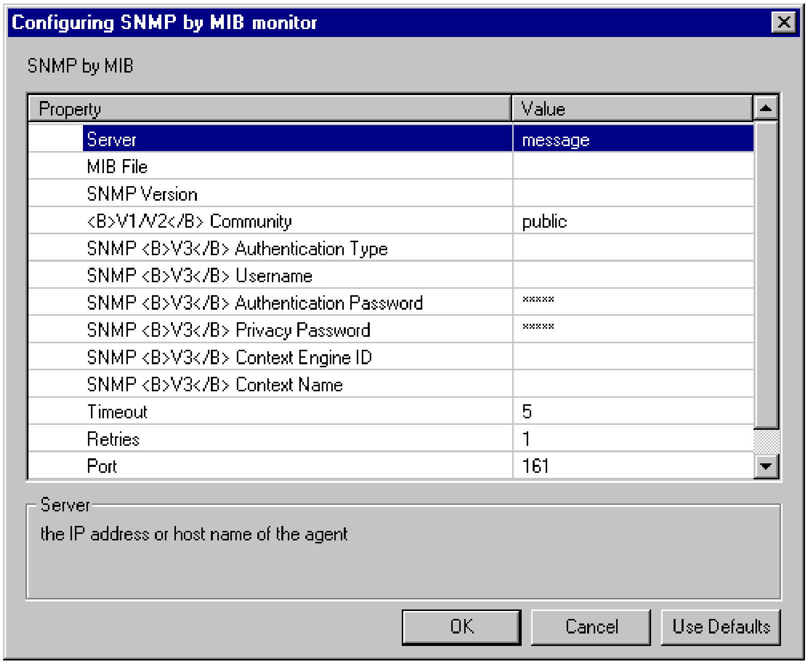
Configuring the SiteScope SNMP by MIB Monitor

After you have added the machine that you are monitoring, you choose the measurements to monitor on the machine.

To configure the SNMP by MIB monitor:

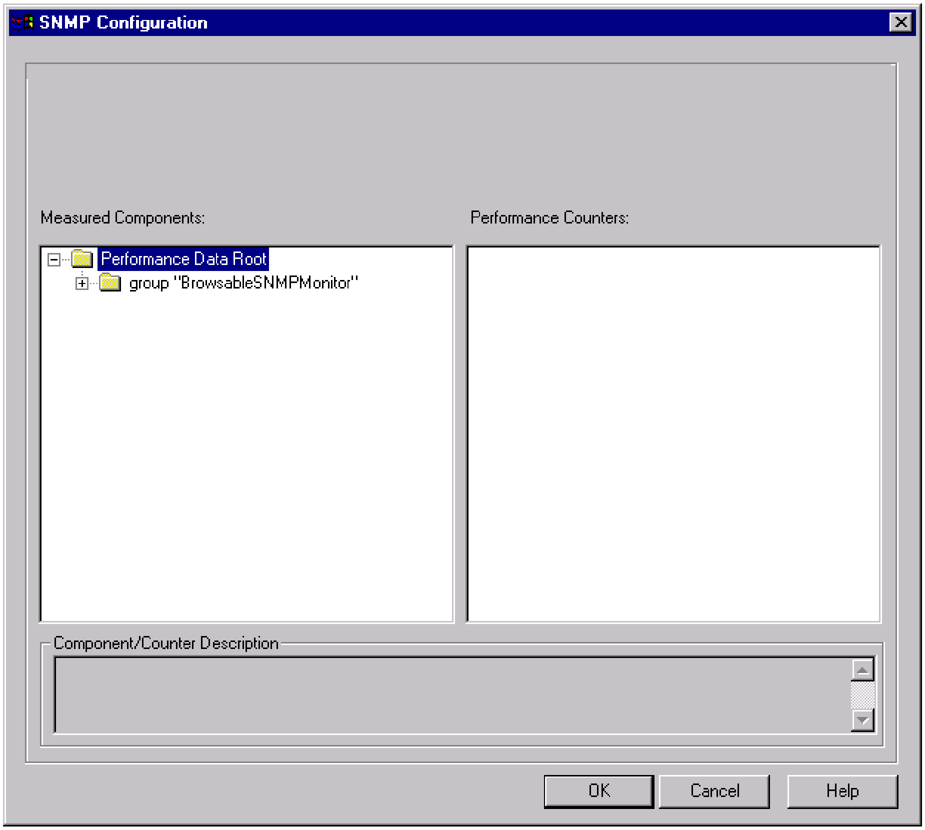
1 The first time you add a measurement to the monitor, you need to configure the monitor properties. When you click **Add** to add a measurement, the Configuring SNMP by MIB Monitor dialog box opens.

Enter values for the monitor properties as described in "Understanding the Configuring SNMP by MIB Monitor Dialog Box" on page 92, and click **OK**.



2 The SNMP Configuration dialog box opens.

Browse the **Measured Components** tree and select the performance counters on the right, as described in "Understanding the SNMP Configuration Dialog Box" on page 93. Click a component or counter to see its description in the **Component/Counter Description** section.



3 Click **OK** to close the SNMP Configuration dialog box. The components that you selected appear in the **Resource Measurements on**: *<machine>* section of the SNMP dialog box.

4 Click **OK** in the SNMP dialog box to activate the monitor.

Note: You can modify the list of resources that you want to monitor at any point during the scenario. A scenario does not have to be active in order for you to monitor the resources on a remote machine.

Understanding the Configuring SNMP by MIB Monitor Dialog Box

You configure the SNMP by MIB monitor in the Configuring SNMP by MIB Monitor dialog box.

➤ **Server.** Enter the name of the server you want to monitor.

➤ **MIB File.** Select the MIB file which contains the objects you are interested in monitoring. If you select a specific MIB file, then only the objects described in that MIB file are displayed. If you select **All MIBs**, then all objects retrieved from the agent during the MIB traversal will be displayed. If no MIB information is available for an object, it is still displayed, but with no textual name or description. To make this monitor aware of new or additional MIBs, simply place new MIB files in the **SiteScope/templates.mib** directory.

➤ **SNMP Version.** Select the version of SNMP to use when connecting.

➤ **V1/V2 Community.** Enter the community string (valid only for version 1 or 2 connections).

➤ **SNMP V3 Authentication Type.** Select the type of authentication to use for version 3 connections.

➤ **SNMP V3 Username.** Enter the username for version 3 connections.

➤ **SNMP V3 Authentication Password.** Enter the authentication password to use for version 3 connections.

➤ **SNMP V3 Privacy Password.** Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.

- **SNMP V3 Context Engine ID.** Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
- **SNMP V3 Context Name.** Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
- **Timeout.** Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. The default is 5 seconds.
- **Retries.** Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. The default is 1 retry.
- **Port.** Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent will typically be listening.
- **Update every.** Enter how frequently the monitor should read the server statistics. The drop-down list to the right of the text box lets you specify time increments of seconds, minutes, hours, or days. You must specify a time increment of at least 3 seconds. The default is 3 seconds.

Understanding the SNMP Configuration Dialog Box

The SNMP Configuration dialog box enables you to select the performance counters to monitor using the Simple Network Management Protocol (SNMP).

- **Host.** The name of the host machine.
- **Measured Components.** Displays a tree containing all the available measured components.
- **Performance Counters.** Displays the performance counters for a selected measured component.
- **Component/Counter Description.** Displays a description of the selected measured component or performance counter.

9

SiteScope Resource Monitoring

The SiteScope Resources monitor graph shows the SiteScope resources measured during the scenario. The SiteScope monitor can measure server, network, and processor performance counters. For detailed information on the performance counters that SiteScope can monitor, refer to the relevant SiteScope documentation.

To obtain data for this graph, you need to select the desired measurements for the online monitor (from the Controller) before running the scenario.

This chapter includes:

Setting up the Monitoring Environment

You select measurements to poll from SiteScope using the SiteScope Monitor Configuration dialog box.

Before setting up the SiteScope monitor:

➤ Ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server. If SiteScope is installed on a machine other than the Controller, verify that the SiteScope machine is accessible from the Controller machine.

Adding a Machine to Monitor

In order to monitor the SiteScope Resources of a particular machine from the Controller, you need to add the machine and the measurements you want to monitor.

To add a machine to the Controller:

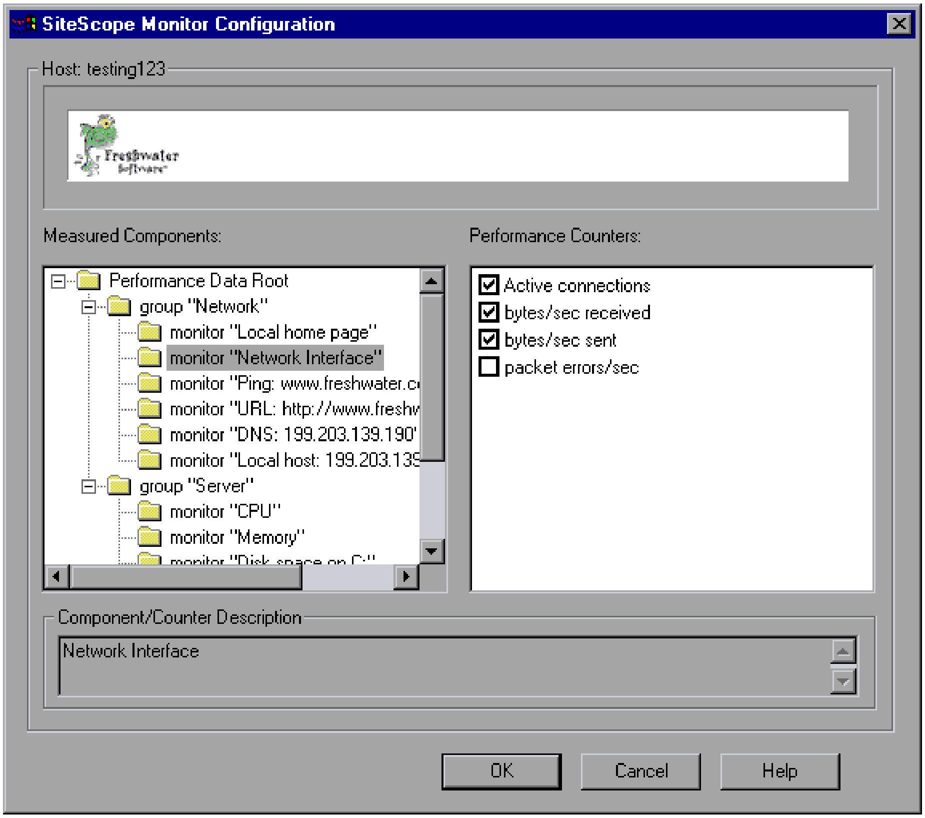
1. Click the SiteScope graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The SiteScope dialog box opens.
3. In the **Monitored Server Machines** section, click **Add**.
4. Enter the server name or IP address of the machine you want to monitor, and select the platform on which the machine runs, and then click **OK**.
5. In the **Resource Measurements** section of the SiteScope dialog box, click **Add**.
6. Continue with "Configuring the SiteScope Monitor" on page 97.

Configuring the SiteScope Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the SiteScope monitor:

1 When you click **Add** in the **Resource Measurements on:** *<machine>* section of the SiteScope dialog box, the SiteScope Monitor Configuration dialog box opens displaying the available measurements.



2 Browse the Measured Components tree, and select performance counters, as described in “Understanding the SiteScope Monitor Configuration Dialog Box” on page 98.

3. Click **OK**. The components that you selected appear in the **Resource Measurements on**: <*machine*> section of the SiteScope dialog box.
4. Click **OK** in the SiteScope Monitor Configuration dialog box, and then in the SiteScope dialog box to activate the monitor.

Note: SiteScope can only be monitored by one Controller at a time.

Understanding the SiteScope Monitor Configuration Dialog Box

Lets you select the items to monitor on the SiteScope application server.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

Part V

Network Delay Monitoring

10

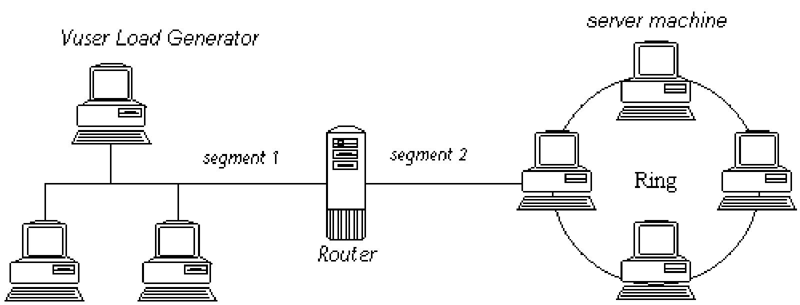
Introduction to Network Monitoring

You use Network monitoring to determine whether your network is causing a delay in the scenario. You can also determine the problematic network segment.

Network configuration is a primary factor in the performance of applications. A poorly designed network can slow client activity to unacceptable levels.

In a true Web or client/server system, there are many network segments. A single network segment with poor performance can affect the entire system.

The following diagram shows a typical network. To go from the server machine to the Vuser machine, data must travel over several segments.



To measure network performance, the Network monitor sends packets of data across the network. When a packet returns, the monitor calculates the time it takes for the packet to go to the requested node and return. This time is the delay which appears in the Network Delay Time graph.

Using the online Network Delay Time graph, you can locate the network-related problem so that it can be fixed.

Note: The delays from the source machine to each of the nodes are measured concurrently, yet independently. It is therefore possible that the delay from the source machine to one of the nodes could be greater than the delay for the complete path between the source and destination machines.

11

Network Delay Monitoring

You use Network Delay monitoring to determine whether your network is causing a delay in the scenario. You can also determine the problematic network segment.

The Network Delay Time monitor shows the delays for the complete path between the source and destination machines (for example the database server and Vuser host). The graph maps the delay as a function of the elapsed scenario time. Each defined path is represented by a separate line with a different color in the graph.

Note: To run the Network monitor, you must have administrator privileges on the Windows source machine (unless you are using the ICMP protocol).

This chapter includes:

Setting up the Monitoring Environment

- You configure the Network monitor from the Run view of the Controller before you begin running a scenario.

Note: To enable network monitoring, you must install the LoadRunner agent on the source machine. You do not have to install the LoadRunner agent on the destination machine.

- You can run the Network monitor on UNIX source machines, using UDP or ICMP. Before running the Network monitor from a UNIX source machine:
  - configure the source machine by assigning root permissions to the **merc_webtrace** process.
  - make the necessary adjustments to either connect to the source machine through RSH, or through the agent.

  This section includes:

- Configuring the Unix Source Machine
- Connecting to the Unix Source Machine Through RSH
- Connecting to the Unix Source Machine Through the Agent

Configuring the Unix Source Machine

You configure the source machine by assigning root permissions to the **merc_webtrace** process.

To configure the source machine, where LoadRunner is installed locally:

1. Log in to the source machine as root.
2. Type: cd <LoadRunner_installation>/bin to change to the **bin** directory.
3. Type: chown root merc_webtrace to make the root user the owner of the **merc_webtrace** file.
4. Type: chmod +s merc_webtrace to add the s-bit to the file permissions.

5 To verify, type ls -l merc_webtrace. The permissions should look like this: -rwsrwsr-x.

To configure the source machine, where LoadRunner is installed on the network:

In a LoadRunner network installation, the **merc_webtrace** process is on the network, not on the source machine disk. The following procedure copies the **merc_webtrace** file to the local disk, configures **mdrv.dat** to recognize the process, and assigns root permissions to **merc_webtrace**:

1 Copy **merc_webtrace** from <**LoadRunner_installation**>**/bin** to anywhere on the local disk of the source machine. For example, to copy the file to the **/local**/<**LoadRunner**> directory, type: cp /net/tools/LoadRunner_installation/bin/merc_webtrace /local/<LoadRunner>

Note: All of the source machines that use the same network installation must copy **merc_webtrace** to the identical directory path on their local disk (for example, /local/<LoadRunner>), since all of them use the same **mdrv.dat**.

---

2 Add the following line to the <**LoadRunner_installation**>**/dat/mdrv.dat** file, in the [monitors_server] section:

```
ExtCmdLine=-merc_webtrace_path /local/xxx
```

3 Log in to the source machine as root.

4 Type: cd LoadRunner_installation/bin to change to the **bin** directory.

5 Type: chown root merc_webtrace to make the root user the owner of the **merc_webtrace** file.

6 Type: chmod +s merc_webtrace to add the s-bit to the file permissions.

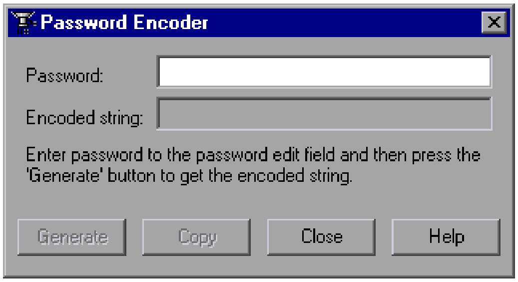
7 To verify, type ls -l merc_webtrace. The permissions should look like: -rwsrwsr-x.

Connecting to the Unix Source Machine Through RSH

If the Controller is connected to the source machine through RSH (default connection mode), you do not need to activate the agent daemon. Before running the Network monitor the first time, you enter an encrypted user name and password in the Network monitor configuration file.

To create an encrypted user name and password:

1 On the Windows taskbar, click **Start**, point to **Programs** > **LoadRunner** > **Tools**, and click **Password Encoder**. The Password Encoder window opens.



2 In the **Password** box, type your RSH user name and password, separated by a vertical bar symbol. For example, myname|mypw.

3 Click **Generate**. An encoded string is displayed in the Encoded string field.

4 Click **Copy** to copy the encoded string to the clipboard.

5 Add the following line to the **<LoadRunner_installation>/dat/monitors/ndm.cfg** file, in the [hosts] section:

Host = <encrypted string copied from clipboard>

6 Close and open the current scenario. LoadRunner will read the updated configuration file and recognize the source machine for monitoring.

Connecting to the Unix Source Machine Through the Agent

If the Controller is not connected to the source machine through RSH, make sure that the agent daemon is active on the source machine before running the Network monitor. For more information about working without RSH, refer to the section titled "UNIX Shell" in Appendix D, "Troubleshooting the Controller" in the *HP LoadRunner Controller User Guide*.

To activate the agent daemon:

If you are not working in RSH, invoke the agent daemon on the source machine.

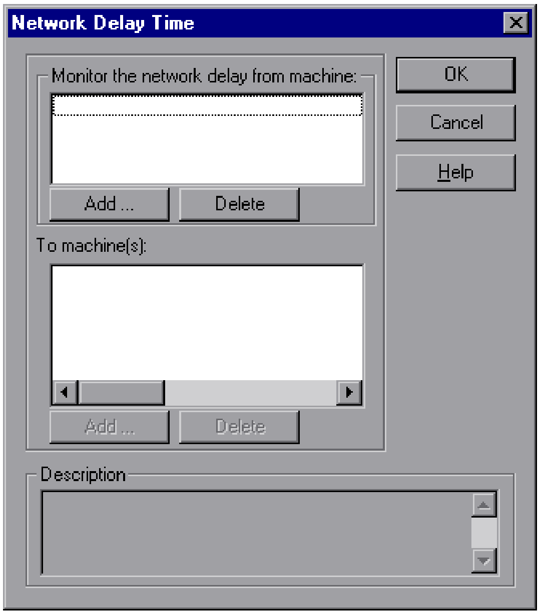
1. Type m_daemon_setup -install from the **<LoadRunner_installation>/bin** directory.
2. Make sure that the agent daemon is running whenever you activate the Network monitor.
3. To stop the Network Delay Monitor agent daemon, type m_daemon_setup -remove.

Adding a Machine to Monitor

In order to monitor the resources of a particular machine you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. In the graph tree view, select the **Network Delay Time** graph and drag it into the right pane.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Network Delay Time dialog box opens.



3. In the **Monitor the network delay from machine** section, click **Add**, and enter the server name or IP address of the source machine, from which you want the network path monitoring to begin. Select the platform on which the machine runs, and click **OK**.

4 In the **To machine(s)** section of the Network Delay Time dialog box, click **Add** to enter the name of the machine at the final destination of the path you want to monitor.

5 Continue with "Configuring the Network Delay Time Monitor" on page 110.

Understanding the Network Delay Time Dialog Box

The Network Delay Time dialog box enables you to select the network path you want to monitor.

Note: To run the Network monitor, you must have administrator privileges on the source machine (unless you are using the ICMP protocol).

- **Monitor the network delay from machine.** Displays the name of the machine from which network monitoring begins. Click **Add** to enter the name of a machine.
  - **Add.** Opens the Add Machine dialog box. Enter the server name or IP address of the source machine, from which you want the network path monitoring to begin. Select the platform on which the machine runs, and click **OK**. Repeat this for each path you want to monitor.
  - **Delete.** Removes the source machine.
- **To machine(s).**
  - **Add.** Opens the Adding Destination Machines for Network Delay Monitoring dialog box.
  - **Delete.** Removes the destination machine.
- **Description.** Displays the name and platform of the highlighted machine.

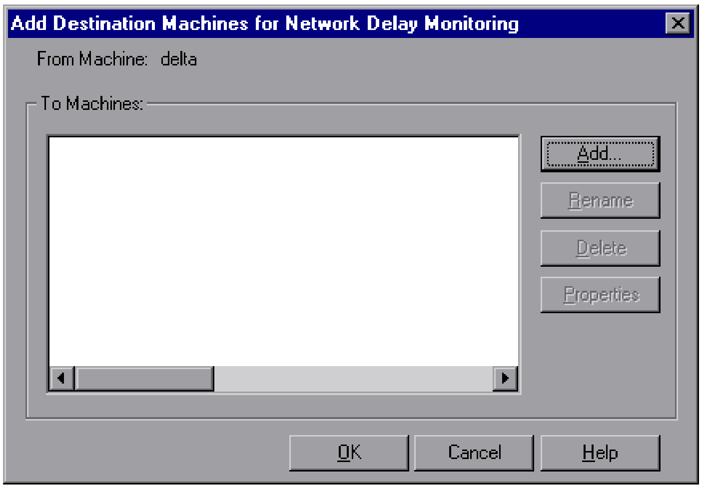
Configuring the Network Delay Time Monitor

You use the Add Destination Machines for Network Delay Monitoring dialog box to configure the Network Delay monitor.

Note: The Network Delay Time Monitor cannot be configured to work in TCP mode on Windows XP SP2 or Vista.

To configure the Network Delay monitor:

1 When you click **Add** in the **To machine(s)** section of the Network Delay Time dialog box, the Add Destination Machines for Network Delay Monitoring dialog box opens.



To add a machine, click **Add**. The New Machine Name dialog box opens.

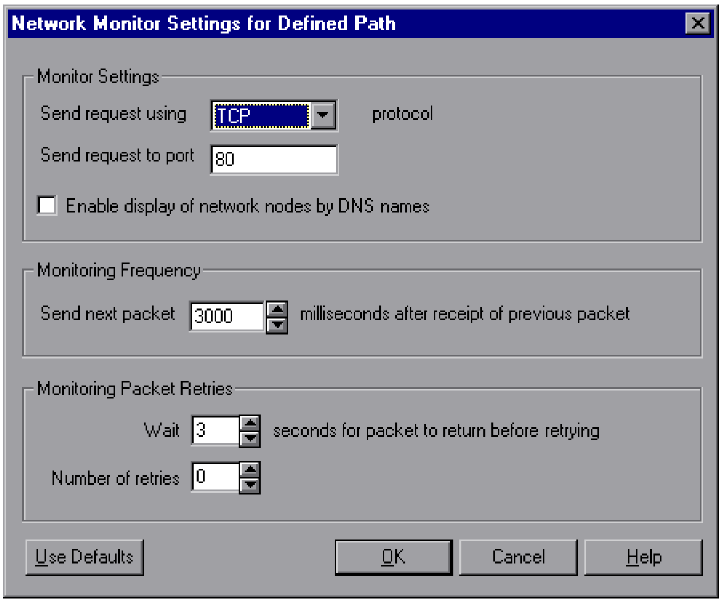
2 Enter the name of the destination machine and click **OK**. The name of the machine appears in the Add Destination Machines for Network Delay Monitoring dialog box. Repeat this procedure for each path you want to monitor, and then click **OK**.

Note: If the destination machine is localhost, enter the local machine's name and not localhost.

➤ To rename a machine, click **Rename**, and enter a new name for the machine.

➤ To delete a machine, select it and click **Delete**.

3 Click **Properties** to configure additional network monitor settings. The Network Monitor Settings for Defined Path dialog box opens.



4 In the Monitor Settings box, select the protocol and enter the port number being used by the network path. The Network monitor supports three protocols: TCP, UDP, and ICMP. It is recommended that you use the default protocol. In Windows, the default is TCP, and in UNIX, the default is UDP.

5 Select **Enable display of network nodes by DNS names** if you want to view the DNS name of each node along the network path, in addition to its IP address.

Note: Selecting this option will decrease the speed of the Network monitor.

---

6 In the Monitoring Frequency box, select the number of milliseconds the monitor should wait between receiving a packet and sending out the next packet. The default value is 3000 milliseconds. If you have a long, steady scenario, you can increase the interval by several seconds.

7 In the Monitoring Packet Retries box, select the maximum number of seconds that the monitor should wait for a packet to return before it retries to send the packet. The default value is 3 seconds. If your network is very large and loaded (an internet connection with a low capacity), you should increase the value by several seconds. If you have a small network (such as a LAN), you can decrease the value.

In addition, select the number of times the Network monitor should try resending a packet to a node if the packet is not initially returned. The default value is 0.

Adding Destination Machines for Network Delay Monitoring Dialog Box

Enables you to add destination machines for network delay monitoring, and configure additional network monitor settings.

- **From Machine.** Displays the name of the source machine.
- **To Machines.** Displays the names or URLs of the destination machines.
- **Add.** Enter the name or URL of the machine at the final destination of the path you want to monitor in the New Machine Name dialog box. Repeat this for each path you want to monitor.
- **Rename.** Renames the destination machine.
- **Delete.** Deletes the destination machine.

- **Properties.** Opens the Configuring Network Monitor Settings for Defined Path dialog box.

Configuring Network Monitor Settings for Defined Path Dialog Box

Lets you set the protocol, port, monitoring frequency, and monitoring packet retries.

- **Monitor Settings.**
  - **Send request using X protocol.** Select the network protocol you want the monitor to use. The Network monitor supports three protocols: TCP, UDP, and ICMP. It is recommended that you use the default protocol, TCP, unless it is necessary for you to use UDP or ICMP.

    Note: When you use TCP or UDP protocols, administrator privileges are required on the source machine.
  - **Send request to port.** Enter the port number to be used by the network path.
  - **Enable display of network nodes by DNS names.** Enables you to view the DNS name of each node along the network path, in addition to its IP address.

    Note: Selecting this option will decrease the speed of the Network monitor.
- **Monitoring Frequency.**
  - **Send next packet X milliseconds after receipt of previous packet.** Select the number of milliseconds the monitor should wait between receiving a packet and sending out the next packet. The default value is 3000 milliseconds.

    Note: If you have a long, steady scenario, you can increase the interval by several seconds.
- **Monitoring Packet Retries.**
  - **Wait X seconds for packet to return before retrying.** Select the maximum number of seconds that the monitor should wait for a packet to return before it retries to send the packet. The default value is 3 seconds.

If your network is very large and loaded (an internet connection with a low capacity), you should increase the value by several seconds. If you have a small network (such as a LAN), you can decrease the value.

- **Number of retries.** Select the number of times the monitor should try resending a packet to a node if the packet is not initially returned. The default value is 0.

- **Use Defaults.** Sets all settings to their default values.

Network Monitoring over a Firewall

If you are monitoring a network in which there are firewalls between the source and the destination machines, you must configure the firewalls to allow the network data packets to reach their destinations.

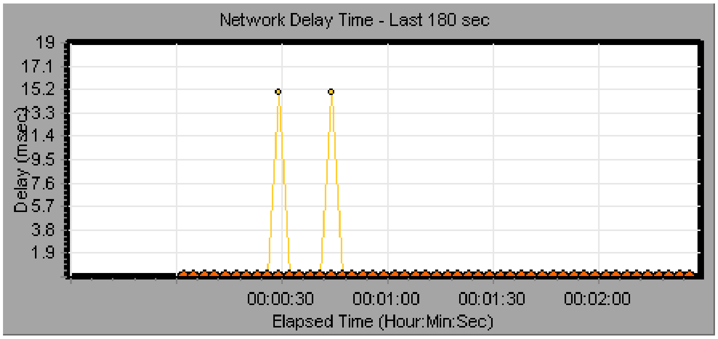
- If you are using the TCP protocol, the firewall that protects the destination machine should not block outgoing ICMP_TIMEEXCEEDED packets (packets that are sent outside the firewall from the machine). In addition, the firewall protecting the source machine should allow ICMP_TIMEEXCEEDED packets to enter, as well as TCP packets to exit.
- If you are using the ICMP protocol, the destination machine's firewall should not block incoming ICMP_ECHO_REQUEST packets, or outgoing ICMP_ECHO_REPLY and ICMP_ECHO_TIMEEXCEEDED packets. In addition, the firewall protecting the source machine should allow ICMP_ECHO_REPLY and ICMP_ECHO_TIMEEXCEEDED packets to enter, and ICMP_ECHO_REQUEST packets to exit.
- If you are using the UDP protocol, ensure that the UDP protocol can access the destination machine from the source machine. The destination machine's firewall should not block outgoing ICMP_DEST_UNREACHABLE and ICMP_ECHO_TIMEEXCEEDED packets. In addition, the firewall protecting the source machine should allow ICMP_DEST_UNREACHABLE and ICMP_ECHO_TIMEEXCEEDED packets to enter.

Note: To run the Network Delay monitor when there are firewalls between the Controller and the source machine, you must configure the LoadRunner agent, MI Listener, and Network Delay monitor for monitoring over a firewall. For more information about configuring LoadRunner Agents inside the firewall, installing and configuring the MI Listener outside the firewall, and configuring the Network Delay monitor over a firewall, see the relevant chapters in the *HP LoadRunner Controller User Guide*.

Viewing the Network Delay Time Graph

The **Network Delay Time** graph shows the delay for the complete path between the source and destination machines (y-axis) as a function of the elapsed scenario time (x-axis).

Each path defined in the Add Destination Machines for Network Delay Monitoring dialog box is represented by a separate line with a different color in the graph.



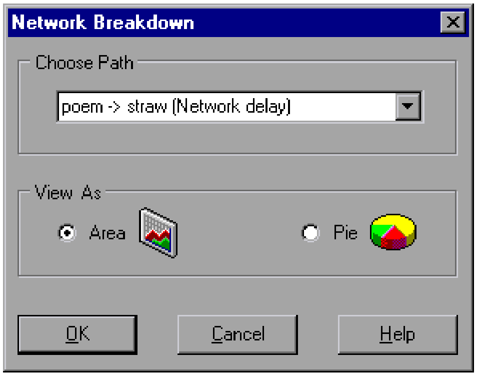
To view the DNS names of the measurements displayed in the legend, right-click the graph and select **View as DNS Name**.

To view the delay time from the source machine to each of the nodes along the network path, right-click the graph and select **Configure**. In the Graph Configuration dialog box, click **SubPaths**.

In addition, you can view the delay time for each segment of the path.

To view the delay time for the network segments:

1. Right-click the Network Delay Time graph, and select **View Segments**. The Network Breakdown dialog box opens.



2. Select the path that you want to break down.
3. Choose whether you want to view the network segments of the graph you chose as an area graph or a pie graph.
4. Click **OK** to close the Network Breakdown dialog box. The delay time for the network segments of the path you chose is displayed in the graph view area.

Note: The segment delays are measured approximately, and do not add up to the network path delay which is measured exactly. The delay for each segment of the path is estimated by calculating the delay from the source machine to one node and subtracting the delay from the source machine to another node. For example, the delay for segment B to C is calculated by measuring the delay from the source machine to point C, and subtracting the delay from the source machine to point B.

To return to the complete path delay time view, select **Hide Segments** from the right-click menu.

Part VI

Firewall Monitoring

12

Firewall Server Performance Monitoring

The Firewall server online monitor measures the performance of a Firewall server during scenario execution, which enables isolation of server performance bottlenecks.

The Check Point FireWall-1 monitor displays statistics about the resource usage on Check Point's FireWall during the scenario run.

This chapter includes:

Setting up the Monitoring Environment

To obtain performance data, you must activate the Firewall server monitor (before executing the scenario) and indicate which statistics and measurements you want to monitor.

Adding a Machine to Monitor

In order to monitor the Check Point FireWall-1 resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the Check Point FireWall-1 graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Check Point FireWall-1 dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

Note: You can specify a machine name and port number in the Add Machine dialog box using the following format:
<machine name>:<port number>

---

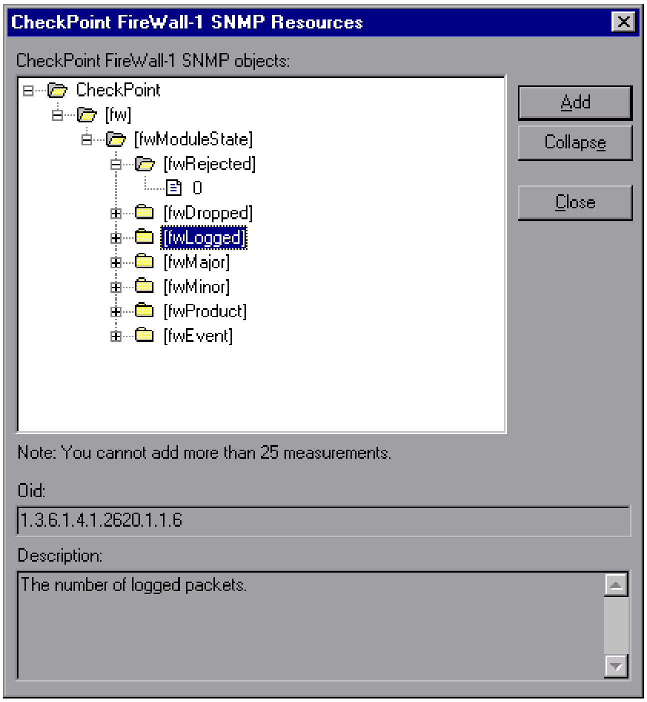
4. In the **Resource Measurements** section of the Check Point FireWall-1 dialog box, click **Add**.
5. Continue with Configuring the Check Point FireWall-1 Server Monitor below.

Configuring the Check Point FireWall-1 Server Monitor

To monitor the Check Point FireWall-1 server, you must select the counters you want the Check Point FireWall-1 server monitor to measure (from the Controller). You select these counters using the Check Point FireWall-1 SNMP Resources dialog box.

To configure the Check Point FireWall-1 server monitor:

1 The Check Point FireWall-1 SNMP Resources dialog box opens.



2 Browse the FireWall-1 Objects list and select the measurements you want to monitor, as described in "Understanding the CheckPoint FireWall-1 Dialog Box" on page 123.

For a description of the available measurements, see "Check Point FireWall-1 Performance Counters" on page 123.

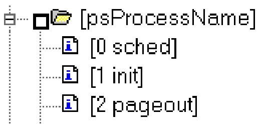
3 Add all the desired resources to the list, and click **Close**.

4 Click **OK** in the Check Point FireWall-1 dialog box to activate the monitor.

Improving the Level of Measurement Information

You can improve the level of measurement information for the Check Point FireWall-1 monitor by enabling measurements with string values to be listed (in addition to measurements with numeric values), and by enabling the name modifier (which displays the string value as an identifying part of the measurement name).

In the following example of a measurement using the name modifier, the string value of ProcessName (sched) is displayed in addition to its instance ID (0):



To enable this feature, add the following line to the <**LoadRunner root folder**>**\dat\monitors\snmp.cfg** file:

```
SNMP_show_string_nodes=1
```

Usage Notes: You can select more than one name modifier, but the first in the hierarchy will be used. Each time the Check Point FireWall-1 Add Measurements dialog box opens, the information is reread from the **snmp.cfg** file. You cannot add the same measurement twice (once with a name modifier and once without it). If you do so, an error message is issued.

Understanding the CheckPoint FireWall-1 Dialog Box

The CheckPoint FireWall-1 dialog box lets you select the CheckPoint FireWall-1 server resources to monitor using the Simple Network Management Protocol (SNMP).

- **CheckPoint FireWall-1 SNMP Objects.** Select each required object and click **Add**. Click **Explain** for the ID number and a description of the selected object.
- **Explain.** Displays a description of the selected object.

Note: The CheckPoint FireWall-1 monitor can only monitor up to 25 measurements.

Check Point FireWall-1 Performance Counters

The following default counters can be monitored:

Measurement	Description
fwRejected	The number of rejected packets.
fwDropped	The number of dropped packets.
fwLogged	The number of logged packets.

Part VII

Web Server Resource Monitoring

13

Introduction to Web Server Resource Monitoring

Using LoadRunner's Web Server Resource monitors, you monitor the Apache, Microsoft IIS, iPlanet (SNMP), and iPlanet/Netscape servers during a scenario run and isolate server performance bottlenecks.

This chapter includes:

About Web Server Resource Monitors

Web Server Resource monitors provide you with information about the resource usage of the Apache, Microsoft IIS, iPlanet (SNMP), and iPlanet/Netscape Web servers during scenario execution. To obtain this data, you need to activate the online monitor for the server and specify which resources you want to measure before executing the scenario.

The procedures for selecting monitor measurements and configuring the monitors vary according to server type. The following sections contain specific configuration instructions for each server type.

Note: Certain measurements or counters are especially useful for determining server performance and isolating the cause of a bottleneck during an initial stress test on a Web server. For more information about these counters, see "Useful Counters for Stress Testing" on page 396.

Monitoring Using a Proxy Server

LoadRunner allows you to monitor using the Apache and Netscape monitors when there is a proxy server between the Controller and the monitored server. To enable this, you must define settings in your configuration file: in <**LoadRunner root folder**>**\dat\monitors\apache.cfg** for the Apache monitor, or in <**LoadRunner root folder**>**\dat\monitors\Netscape.cfg** for the Netscape monitor.

Before defining settings, you need to determine whether you want LoadRunner to obtain proxy settings from your Internet Explorer connection configuration, or from the proxy settings in the configuration file.

To have LoadRunner read proxy settings from your Internet Explorer connection:

1 In the Proxy Settings section of the configuration file, assign **useProxy** a value of 1.

2 If the proxy requires a username, password, or domain, enter these parameters on the lines **proxyUsername**, **proxyPassword**, and **proxyDomain**.

To have LoadRunner read proxy settings from the configuration file:

1 In the Proxy Settings section of the configuration file, enter the proxy information on the **httpProxy** line. Use the format:
[<protocol>=][<scheme>://]<proxy>[:<port>][[<protocol>=][<scheme>://]<proxy>[:<port>]]

For example:

```
httpProxy=http=http://my_http_proxy:8080 https=https://my_https_proxy:9000
```

2 If the proxy requires a username, password, or domain, enter these parameters on the lines **proxyUsername**, **proxyPassword**, and **proxyDomain**.

To have LoadRunner connect directly to the server (any proxy settings are ignored):

➤ In the Proxy Settings section of the configuration file, assign **useProxy** a value of 0.

14

iPlanet/Netscape Monitoring

This Web Server Resource monitor displays statistics about the resource usage on the iPlanet/Netscape Web server during the scenario run.

To obtain data for this graph, you need to configure the iPlanet/Netscape online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

This chapter includes:

Setting up the Monitoring Environment

To monitor an iPlanet/Netscape server, you need to know the administration server URL. A simple way to verify the administration server URL, is to try to view it through the browser.

The URL should be in the following format:

```
http://<admin_srv_name/IP address>:<port number>/https-<admin_srv_name/
IP address>/bin/sitemon?doit
```

For example:

```
http://lazarus:12000/https-lazarus.HP.co.il/bin/sitemon?doit
```

Note: In some server configurations, the URL must contain the administration server name and not the IP address.

In addition, the administration server name may differ from the iPlanet/Netscape server name.

Adding a Machine to Monitor

In order to monitor the iPlanet/Netscape resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the iPlanet/Netscape graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The iPlanet/Netscape dialog box opens.

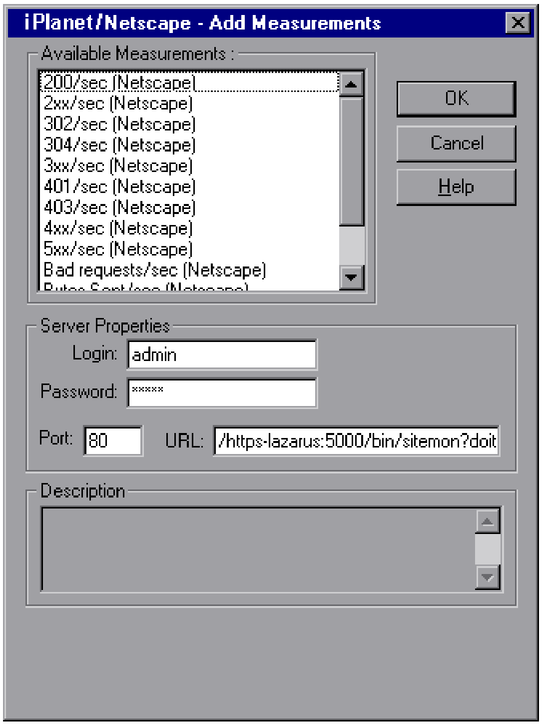
   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.
4. In the **Resource Measurements** section of the iPlanet/Netscape dialog box, click **Add**.
5. Continue with “Configuring the iPlanet/Netscape Monitor” on page 132.

Configuring the iPlanet/Netscape Monitor

To obtain data for this graph, you need to configure the iPlanet/Netscape online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

To configure the iPlanet/Netscape monitor:

1 The iPlanet/Netscape - Add Measurements dialog box opens, displaying the available measurements and server properties.



Select the required measurements.

For a description of the available measurements, see “iPlanet/Netscape Performance Counters” on page 135.

2 Fill in the Server Properties:

➤ Enter the user login name and password. The user must have administrator permissions on the server.

- Enter the port number and URL (without the server name), and click **OK**. The default URL is /https-<admin_server>/bin/sitemon?doit.

3 Click **OK** in the iPlanet/Netscape - Add Measurements dialog box and in the iPlanet/Netscape dialog box to activate the monitor.

Understanding the iPlanet/Netscape Dialog Box

The iPlanet/Netscape dialog box lets you select the items to monitor on the iPlanet/Netscape server.

- **Available Measurements.** Select the required measurements. Select multiple measurements using the CTRL key. A description of the selected measurement appears in the Description box.
- **Server Properties.**
  - **Login.** Enter the user login name. The user must have administrator permissions on the server.
  - **Password.** Enter the user password.
  - **Port.** Enter the server's port number.
  - **URL.** To monitor an iPlanet/Netscape server, you need to know the server statistics information URL. A simple way to verify the statistics information URL is to try to view it through the browser.

    The URL should be in the following format:

    http://<admin_srv_name/IP address>:<port number>/https-<admin_srv_name/IP address>/bin/sitemon?doit

    For example:

    http://lazarus:80/https-lazarus/bin/sitemon?doit

    Enter the server's URL, without the server name. The default URL is /https-<server>/bin/sitemon?doit.

Note: The default port number and URL can vary from one server to another. Please consult the Web server administrator. In some server configurations, the URL must contain the server name and not the IP address.

- **Description.** Displays a description of the selected measurement.

iPlanet/Netscape Performance Counters

The following table describes the measurements and server properties that can be monitored:

Measurement	Description
200/sec	The rate of successful transactions being processed by the server
2xx/sec	The rate at which the server handles status codes in the 200 to 299 range
302/sec	The rate of relocated URLs being processed by the server
304/sec	The rate of requests for which the server tells the user to use a local copy of a URL instead of retrieving a newer version from the server
3xx/sec	The rate at which the server handles status codes in the 300 to 399 range
401/sec	The rate of unauthorized requests handled by the server
403/sec	The rate of forbidden URL status codes handled by the server
4xx/sec	The rate at which the server handles status codes in the 400 to 499 range
5xx/sec	The rate at which the server handles status codes 500 and higher
Bad requests/sec	The rate at which the server handles bad requests
Bytes sent/sec	The rate at which bytes of data are sent from the Web server
Hits/sec	The HTTP request rate
xxx/sec	The rate of all status codes (2xx-5xx) handled by the server, excluding timeouts and other errors that did return an HTTP status code

To change the default server properties:

1. Open the **Netscape.cfg** file in the **<LoadRunner root folder>\dat\monitors** directory.
2. Edit the following parameters in the [Netscape] section:

Counters	number of counters that the LoadRunner iPlanet/Netscape monitor will show you. This value should match the number of counters defined in the file.
InfoURL	server statistics information URL
ServerPort	server port number
ServerLogin	login name to the server
ServerPassword	login password for the login name
SamplingRate	rate (milliseconds) at which the LoadRunner monitor will poll the server for the statistics information. If this value is greater than 1000, LoadRunner will use it as its sampling rate. Otherwise, it will use the sampling rate defined in the Monitors tab of the Options dialog box.

Note: To monitor an iPlanet/Netscape server through a firewall, use the iPlanet/Netscape Administration server port. Configure this port during the server installation process.

15

iPlanet (SNMP) Monitoring

This Web Server Resource monitor displays statistics about the resource usage on the iPlanet (SNMP) Web server during the scenario run. The iPlanet (SNMP) monitor uses the Simple Network Management Protocol (SNMP) to retrieve iPlanet (SNMP) server statistics.

To obtain data for this graph, you need to configure the iPlanet (SNMP) online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You define the measurements for the iPlanet (SNMP) monitor using the iPlanet (SNMP) dialog box.

Note: To monitor a iPlanet (SNMP) server, use port 161 or 162, depending on the configuration of the agent.

This chapter includes:

Adding a Machine to Monitor

In order to monitor the iPlanet (SNMP) resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the iPlanet (SNMP) graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The iPlanet (SNMP) dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

Note: If the iPlanet SNMP agent is running on a different port than the default SNMP port, you need to define the port number. Enter the following information in the Add Machine dialog box:
<server name:port number>

For example: digi:8888

In addition, you can define the default port for your iPlanet server in the configuration file, **snmp.cfg**, located in <**LoadRunner root folder**>**\dat\monitors**. For example, if the port used by the SNMP agent on your iPlanet server is 8888, you should edit the **snmp.cfg** file as follows:
; iPlanet (WebServer)
[cm_snmp_mon_iws60]
port=8888

---

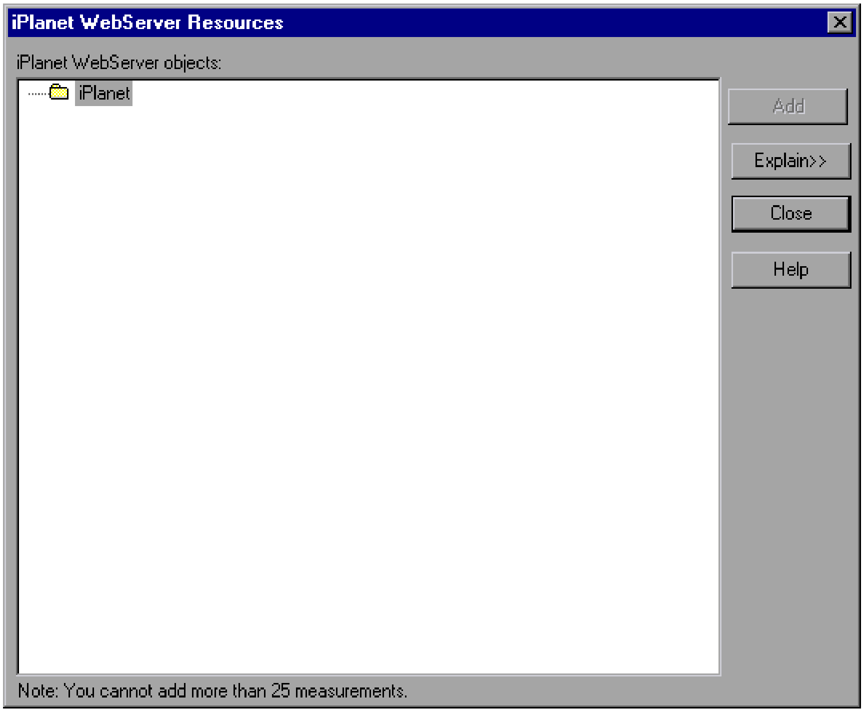
4. In the **Resource Measurements** section of the iPlanet (SNMP) dialog box, click **Add**.
5. Continue with "Configuring the iPlanet (SNMP) Monitor" on page 139.

Configuring the iPlanet (SNMP) Monitor

Before running the scenario, you need to select the measurements you want to display on the iPlanet (SNMP) monitor.

To configure the iPlanet (SNMP) monitor:

1 When you click **Add** to add a measurement to monitor, the iPlanet WebServer Resources dialog box opens.



Browse the **iPlanet WebServer Object** tree as described in "Understanding the iPlanet (SNMP) Dialog Box" on page 141, and select performance counters.

For a description of the available measurements, see "iPlanet (SNMP) Performance Counters" on page 141.

Note: The iPlanet (SNMP) monitor can only monitor up to 25 measurements.

---

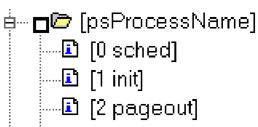
2 Add all the desired resources to the list, and click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the iPlanet (SNMP) dialog box.

3 Click **OK** in the iPlanet (SNMP) dialog box to activate the monitor.

Improving the Level of Measurement Information

You can improve the level of measurement information for the iPlanet (SNMP) monitor by enabling measurements with string values to be listed (in addition to measurements with numeric values), and by enabling the name modifier (which displays the string value as an identifying part of the measurement name).

In the following example of a measurement using the name modifier, the string value of ProcessName (sched) is displayed in addition to its instance ID (0):



To enable this feature, add the following line to the <**LoadRunner root folder**>**\dat\monitors\snmp.cfg** file:

```
SNMP_show_string_nodes=1
```

Usage Notes: You can select more than one name modifier, but the first in the hierarchy will be used. Each time the iPlanet SNMP Add Measurements dialog box opens, the information is reread from the **snmp.cfg** file. You cannot add the same measurement twice (once with a name modifier and once without it). If you do so, an error message is issued.

Understanding the iPlanet (SNMP) Dialog Box

The iPlanet (SNMP) dialog box lets you select the iPlanet (SNMP) server resources to monitor using the Simple Network Management Protocol (SNMP).

➤ **iPlanet (SNMP) Objects.** Select each required object and click **Add**. Click **Explain** for the ID number and a description of the selected object.

➤ **Explain.** Displays a description of the selected object.

Note: The iPlanet (SNMP) monitor can only monitor up to 25 measurements.

---

iPlanet (SNMP) Performance Counters

The following table describes the measurements and server properties that can be monitored:

Measurement	Description
iwsInstanceTable	iPlanet Web Server instances
iwsInstanceEntry	iPlanet Web Server instances
iwsInstanceIndex	Server instance index
iwsInstanceId	Server instance identifier
iwsInstanceVersion	Server instance software version
iwsInstanceDescription	Description of server instance
iwsInstanceOrganization	Organization responsible for server instance
iwsInstanceContact	Contact information for person(s) responsible for server instance
iwsInstanceLocation	Location of server instance
iwsInstanceStatus	Server instance status

Measurement	Description
iwsInstanceUptime	Server instance uptime
iwsInstanceDeathCount	Number of times server instance processes have died
iwsInstanceRequests	Number of requests processed
iwsInstanceInOctets	Number of octets received
iwsInstanceOutOctets	Number of octets transmitted
iwsInstanceCount2xx	Number of 200-level (Successful) responses issued
iwsInstanceCount3xx	Number of 300-level (Redirection) responses issued
iwsInstanceCount4xx	Number of 400-level (Client Error) responses issued
iwsInstanceCount5xx	Number of 500-level (Server Error) responses issued
iwsInstanceCountOther	Number of other (neither 2xx, 3xx, 4xx, nor 5xx) responses issued
iwsInstanceCount200	Number of 200 (OK) responses issued
iwsInstanceCount302	Number of 302 (Moved Temporarily) responses issued
iwsInstanceCount304	Number of 304 (Not Modified) responses issued
iwsInstanceCount400	Number of 400 (Bad Request) responses issued
iwsInstanceCount401	Number of 401 (Unauthorized) responses issued
iwsInstanceCount403	Number of 403 (Forbidden) responses issued
iwsInstanceCount404	Number of 404 (Not Found) responses issued
iwsInstanceCount503	Number of 503 (Unavailable) responses issued
iwsInstanceLoad 1MinuteAverage	System load average for 1 minute

Measurement	Description
iwsInstanceLoad 5MinuteAverage	System load average for 5 minutes
iwsInstanceLoad 15MinuteAverage	System load average for 15 minutes
iwsInstanceNetwork InOctets	Number of octets transmitted on the network per second
iwsInstanceNetwork OutOctets	Number of octets received on the network per second
iwsVsTable	iPlanet Web Server virtual servers
iwsVsEntry	iPlanet Web Server virtual server
iwsVsIndex	Virtual server index
iwsVsId	Virtual server identifier
iwsVsRequests	Number of requests processed
iwsVsInOctets	Number of octets received
iwsVsOutOctets	Number of octets transmitted
iwsVsCount2xx	Number of 200-level (Successful) responses issued
iwsVsCount3xx	Number of 300-level (Redirection) responses issued
iwsVsCount4xx	Number of 400-level (Client Error) responses issued
iwsVsCount5xx	Number of 500-level (Server Error) responses issued
iwsVsCountOther	Number of other (neither 2xx, 3xx, 4xx, nor 5xx) responses issued
iwsVsCount200	Number of 200 (OK) responses issued
iwsVsCount302	Number of 302 (Moved Temporarily) responses issued
iwsVsCount304	Number of 304 (Not Modified) responses issued

Measurement	Description
iwsVsCount400	Number of 400 (Bad Request) responses issued
iwsVsCount401	Number of 401 (Unauthorized) responses issued
iwsVsCount403	Number of 403 (Forbidden) responses issued
iwsVsCount404	Number of 404 (Not Found) responses issued
iwsVsCount503	Number of 503 (Unavailable) responses issued
iwsProcessTable	iPlanet Web Server processes
iwsProcessEntry	iPlanet Web Server process
iwsProcessIndex	Process index
iwsProcessId	Operating system process identifier
iwsProcessThreadCount	Number of request processing threads
iwsProcessThreadIdle	Number of request processing threads currently idle
iwsProcessConnection QueueCount	Number of connections currently in connection queue
iwsProcessConnection QueuePeak	Largest number of connections that have been queued simultaneously
iwsProcessConnection QueueMax	Maximum number of connections allowed in connection queue
iwsProcessConnection QueueTotal	Number of connections that have been accepted
iwsProcessConnection QueueOverflows	Number of connections rejected due to connection queue overflow
iwsProcessKeepalive Count	Number of connections currently in keepalive queue
iwsProcessKeepaliveMax	Maximum number of connections allowed in keepalive queue
iwsProcessSizeVirtual	Process size in kbytes
iwsProcessSizeResident	Process resident size in kbytes

Measurement	Description
iwsProcessFraction SystemMemoryUsage	Fraction of process memory in system memory
iwsListenTable	iPlanet Web Server listen sockets
iwsListenEntry	iPlanet Web Server listen socket
iwsListenIndex	Listen socket index
iwsListenId	Listen socket identifier
iwsListenAddress	Address socket is listening on
iwsListenPort	Port socket is listening on
iwsListenSecurity	Encryption support
iwsThreadPoolTable	iPlanet Web Server thread pools
iwsThreadPoolEntry	iPlanet Web Server thread pool
iwsThreadPoolIndex	Thread pool index
iwsThreadPoolId	Thread pool identifier
iwsThreadPoolCount	Number of requests queued
iwsThreadPoolPeak	Largest number of requests that have been queued simultaneously
iwsThreadPoolMax	Maximum number of requests allowed in queue
iwsCpuTable	iPlanet Web Server CPUs
iwsCpuEntry	iPlanet Web Server CPU
iwsCpuIndex	CPU index
iwsCpuId	CPU identifier
iwsCpuIdleTime	CPU Idle Time
iwsCpuUserTime	CPU User Time
iwsCpuKernelTime	CPU Kernel Time

16

Microsoft IIS Monitoring

This Web Server Resource monitor displays statistics about the resource usage on the Microsoft Internet Information Server (IIS) during the scenario run.

To obtain data for this graph, you need to configure the MS IIS online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You select measurements for the Microsoft IIS Server monitor using the MS IIS dialog box.

Note: To monitor an IIS server through a firewall, use TCP, port 139.

This chapter includes:

Adding a Machine to Monitor

In order to monitor the Microsoft_IIS server from the Controller, you need to add the machine and the measurements you want to monitor.

To add a machine to the Controller:

1. Click the MS IIS graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The MS IIS dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.
4. In the **Resource Measurements on:** <*machine*> section of the MS-IIS dialog box, the default measurements are displayed.
   - To delete a measurement from the default list, select the measurement and click **Delete**.
   - To select additional measurements, click **Add**. A dialog box opens displaying all the available measurements.

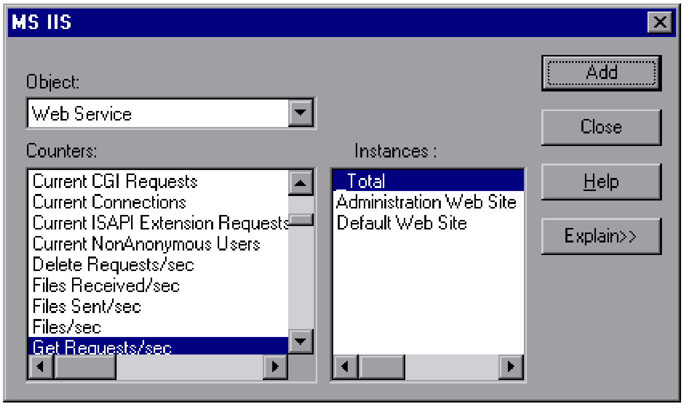
     For a description of the available measurements, see "Microsoft IIS Performance Counters" on page 151.

     Note: To change the default counters for the Microsoft IIS Server monitor, see "Changing a Monitor's Default Counters" on page 395.
5. Continue with Configuring the Microsoft IIS Monitor below.

Configuring the Microsoft IIS Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which objects to monitor on the machine.

1 When you click **Add** to add a measurement, the MS IIS dialog box opens displaying the Web Service object, its counters, and instances opens.



For each measurement, select an object, counter, and instance, and then click **Add**, as described in “Understanding the MS IIS Dialog Box” on page 150.

For a description of the available measurements, see “Microsoft IIS Performance Counters” on page 151.

Note: To change the default counters for the Microsoft IIS Server monitor, see “Changing a Monitor’s Default Counters” on page 395.

---

2 Add all the desired resources to the list, and click **Close**.

3 Click **OK** in the MS IIS dialog box to activate the monitor.

Understanding the MS IIS Dialog Box

The MS IIS dialog box lets you select the items to monitor on the MS IIS server.

➤ **Object.** Select the object being monitored on the specified machine.

➤ **Counters.** Select a resource counter to monitor. Select multiple counters using the CTRL key. For an explanation of each counter, click **Explain**.

➤ **Instances.** If multiple instances of the selected counter are running, select one or more instances to monitor for the selected counter.

➤ **Explain.** Displays a description of the selected counter.

Microsoft IIS Performance Counters

The following table describes the default measurements that can be monitored:

Object	Measurement	Description
Web Service	**Bytes Sent/sec**	The rate at which the data bytes are sent by the Web service
Web Service	**Bytes Received/sec**	The rate at which the data bytes are received by the Web service
Web Service	**Get Requests/sec**	The rate at which HTTP requests using the GET method are made. Get requests are generally used for basic file retrievals or image maps, though they can be used with forms.
Web Service	**Post Requests/sec**	The rate at which HTTP requests using the POST method are made. Post requests are generally used for forms or gateway requests.
Web Service	**Maximum Connections**	The maximum number of simultaneous connections established with the Web service
Web Service	**Current Connections**	The current number of connections established with the Web service
Web Service	**Current NonAnonymous Users**	The number of users that currently have a non-anonymous connection using the Web service
Web Service	**Not Found Errors/sec**	The rate of errors due to requests that could not be satisfied by the server because the requested document could not be found. These are generally reported to the client as an HTTP 404 error code.
Process	**Private Bytes**	The current number of bytes that the process has allocated that cannot be shared with other processes.

Part VIII

Web Application Server Monitoring

17

Introduction to Web Application Server Resource Monitoring

You use LoadRunner's Web Application Server Resource monitors to monitor Web application servers during a scenario run and isolate application server performance bottlenecks.

Web Application Server Resource monitors provide you with information about the resource usage of the Ariba, ATG Dynamo, BroadVision, ColdFusion, Fujitsu INTERSTAGE, iPlanet (NAS), Microsoft ASP, Oracle9iAS HTTP, SilverStream, WebLogic (SNMP), WebLogic (JMX), and WebSphere application servers during scenario execution. To obtain performance data, you need to activate the online monitor for the server and specify which resources you want to measure before executing the scenario.

The procedures for selecting monitor measurements and configuring the monitors vary according to server type. The following sections contain specific configuration instructions for each server type.

18

Ariba Monitoring

The Ariba monitor displays statistics about the resource usage on the Ariba server during the scenario run.

To obtain data for this graph, you need to configure the Ariba online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You select measurements to monitor the Ariba server using the Ariba Monitor Configuration dialog box.

Note: The port you use to monitor an Ariba server through a firewall depends on the configuration of your server.

This chapter includes:

Adding a Machine to Monitor

In order to monitor the Ariba resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the Ariba graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Ariba dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor according to the following format: <server name>:<port number>.

   For example: merc1:12130

   Select the platform on which the machine runs, and click **OK**.
4. In the **Resource Measurements** section of the Ariba dialog box, click **Add**.

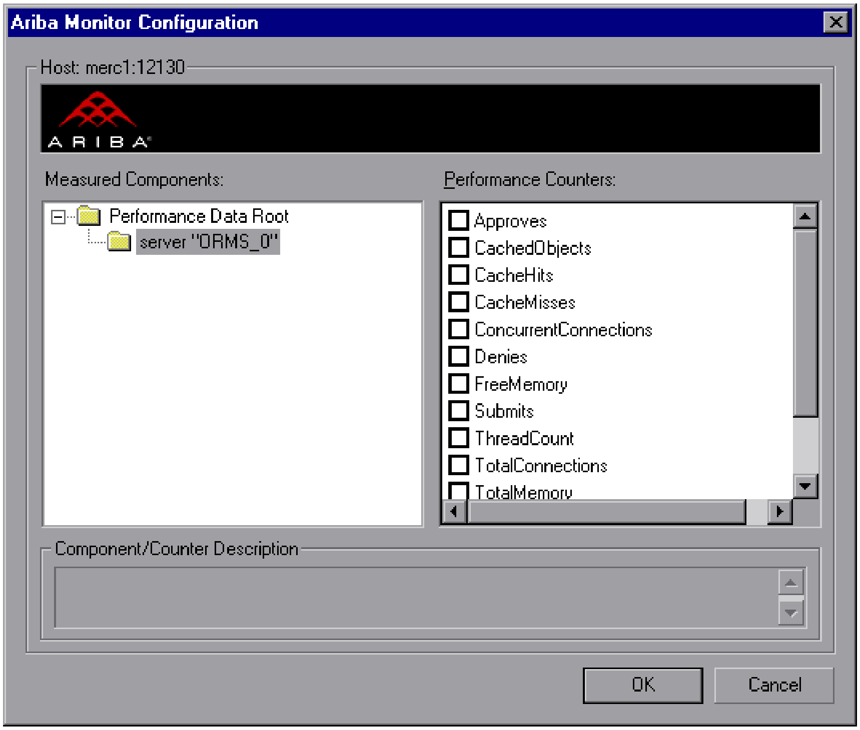
   Continue with Configuring the Ariba Monitor below.

Configuring the Ariba Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which objects to monitor on the machine.

To configure the Ariba monitor:

1 When you click **Add** to add a measurement, the Ariba Monitor Configuration dialog box opens.



Browse the Measured Components tree, and select performance counters as described in "Understanding the Ariba Monitor Configuration Dialog Box" on page 160.

For a description of the available measurements, see "Ariba Performance Counters" on page 161.

2 Click **OK** in the Ariba Monitor Configuration dialog box, and in the Ariba dialog box, to activate the Ariba monitor.

XML Accessibility Verification

Only browsers that are XML-compatible will allow you to view the performance XML file.

To verify whether the XML file is accessible:

Display the XML file through the browser. The URL should be in the following format: http://<server name:port number>/metrics?query=getStats

For example: http://merc1:12130/metrics?query=getStats

Note: In some cases, although the browser is XML-compatible, it may still return the error: The XML page cannot be displayed. In these cases, the XML file can be accessed by the Ariba performance monitor, although it cannot be viewed by the browser.

Understanding the Ariba Monitor Configuration Dialog Box

The Ariba dialog box lets you select the items to monitor on the Ariba application server.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

Note: Only browsers that are XML-compatible will allow you to view the performance XML file.

To verify whether the XML file is accessible, display the XML file through the browser. The URL should be in the following format: http://<server name:server port>/metrics?query=getStats

For example: http://merc1:12130/metrics?query=getStats

Ariba Performance Counters

The following tables describe the counters that can be monitored:

Core Server Performance Counters

The following counters measure Core Server Performance:

Measurement	Description
Total Connections	The cumulative number of concurrent user connections since Ariba Buyer was started.
Requisitions Finished	The instantaneous reading of the length of the worker queue at the moment this metric is obtained. The longer the worker queue, the more user requests are delayed for processing.
Worker Queue Length	The instantaneous reading of the length of the worker queue at the moment this metric is obtained. The longer the worker queue, the more user requests are delayed for processing.
Concurrent Connections	The instantaneous reading of the number of concurrent user connections at the moment this metric is obtained.
Total Memory	The instantaneous reading of the memory (in KB) being used by Ariba Buyer at the moment this metric is obtained.

Measurement	Description
Free Memory	The instantaneous reading of the reserved memory (in bytes) that is not currently in use at the moment this metric is obtained.
Up Time	The amount of time (in hours and minutes) that Ariba Buyer has been running since the previous time it was started.
Number of Threads	The instantaneous reading of the number of server threads in existence at the moment this metric is obtained.
Number of Cached Objects	The instantaneous reading of the number of Ariba Buyer objects being held in memory at the moment this metric is obtained.
Average Session Length	The average length of the user sessions (in seconds) of all users who logged out since previous sampling time. This value indicates how long, on average, a user stays connected to server.
Average Idle Time	The average idle time (in seconds) for all the users who have been active since previous sampling time. The idle time is the period of time between two consecutive user requests from the same user.
Approves	The cumulative count of the number of Approves that occurred during the sampling period. An Approve consists of a user approving one Approvable.
Submits	The cumulative count of the number of Approvals submitted since previous sampling time.
Denies	The cumulative count of the number of submitted Approvals denied since previous sampling time.
Object Cache Accesses	The cumulative count of accesses (both reads and writes) to the object cache since previous sampling time.
Object Cache Hits	The cumulative count of accesses to the object cache that are successful (cache hits) since previous sampling time.

System Related Performance Counters

The following counters measure System Related Performance:

Measurement	Description
Database Response Time	The average response time (in seconds) to the database requests since the previous sampling time.
Buyer to DB server Traffic	The cumulative number of bytes that Ariba Buyer sent to the DB server since the previous sampling time.
DB to Buyer server Traffic	The cumulative number of bytes that the DB server sent to Ariba Buyer since the previous sampling time.
Database Query Packets	The average number of packets that Ariba Buyer sent to the DB server since the previous sampling time.
Database Response Packets	The average number of packets that the DB server sent to Ariba Buyer since the previous sampling time.

19

iPlanet (NAS) Monitoring

This Web Application Server Resource displays statistics about the resource usage on the iPlanet (NAS) Web application server during the scenario run. The iPlanet (NAS) monitor uses the SNMP to retrieve iPlanet (NAS) server statistics.

To obtain data for this graph, you must first configure the iPlanet SNMP Service on the application server. You can then enable the iPlanet (NAS) online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You define the measurements for the iPlanet (NAS) monitor using the iPlanet (NAS) dialog box.

This chapter includes:

Setting Up the Monitoring Environment

Before you can configure the monitor, you need to set up the application server for SNMP monitoring.

This section offers a short explanation on setting up SNMP monitoring of the iPlanet Application Server. It is intended to supplement the iPlanet documentation, not act as a replacement. For an explanation of the SNMP reporting architecture and theory, refer to the iPlanet documentation.

Note: The instructions below assume that SNMP statistics will be collected on the standard SNMP port 161.

SNMP Summary

- Solaris has a native SNMP agent, **snmpdx**, that is started automatically at boot time by the script **/etc/rc3.d/S76snmpdx**. This daemon communicates on the standard SNMP port 161. The port number can be changed with the -p <port> option.
- Planet Products are shipped with their own SNMP agents. The architecture is such that there is one "master agent" per host, which a network management station communicates with, and one or more "subagents" that collect data from various iPlanet products and forward statistics to the master agent. The master agent also defaults to communicating on port 161.
- To run both the Solaris SNMP agent and the iPlanet SNMP agent, a proxy must be used that makes the Sun agent look like a subagent to the iPlanet master agent.

Steps Overview

- Login to the system as root
- Change the port number for the Solaris SNMP agent
- Configure and run the iPlanet agents "magt" and "sagt"
- Start the Solaris SNMP agent
- Configure iPlanet Application Server for SNMP statistics
- Start SNMP subagents for iPlanet Directory Server and iPlanet Web Server (optional)

Changing the Port Number for the Solaris SNMP Agent

1. Login to the system as root. (Only a root user can change the port number and run the agents).
2. Stop the SNMP agent by running /etc/rc2.d/K76snmpdx stop.
3. Edit /etc/rc3.d/S76snmpdx to run the Solaris daemon on a non-standard port number. For example, 1161:
   Replace
   /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf
   with
   /usr/lib/snmp/snmpdx -p 1161 -y -c /etc/snmp/conf

Configuring and Running the iPlanet Agents

The master and proxy agents and startup scripts are found in <**ias install directory**>**\snmp**.

1. In the script S75snmpagt, add a line to the environment variable GX_ROOTDIR so that it points to your iAS installation. For example, if the iPlanet Application Server is installed in /usr/iplanet/ias6/ias:

   GX_ROOTDIR=/usr/iplanet/ias6/ias
   exprt GX_ROOTDIR
2. Copy the script S75snmpagt to /etc/rc3.d
3. chmod 755 /etc/rc3.d/S75snmpagt
4. In /etc/rc3.d/S75snmpagt /etc/rc2.d/K07snmpagt

5 You can configure system information and traps.

In the example below, information has been added about the system owner and location, and SNMP traps have been sent to a network manager station ("mde.uk.sun.com").

```
COMMUNITY       public
ALLOW ALL OPERATIONS
INITIAL sysLocation "Under Joe Bloggs' Desk in Headquarters"
INITIAL sysContact "Joe Bloggs
Email: Joe.Bloggs@Sun.COM
Voice: +1 650 555 1212"
MANAGER mde.uk.sun.com
SEND ALL TRAPS TO PORT 162
WITH COMMUNITY public
```

Note: There is no need to edit the proxy agent's configuration file (CONFIG_SAGT).

---

6 Start the iPlanet agents by running the command:
/etc/rc3.d/S75snmpagt start

To start the Solaris SNMP agent:

Restart the Solaris SNMP agent by running the command:
/etc/rc3.d/S76snmpdx start

Configuring the iPlanet Application Server for SNMP Statistics

1 Start the iPlanet Application Server admin tool ksvradmin.

2 In the General View, select the instance name that you want to manage.

3 Click the **SNMP** tab in the management frame.

4 Select **Enable SNMP Administration and Monitoring** and **Enable SNMP Debug**.

5 Type 60 in the Connection Attempt Interval field, and exit ksvradmin.

6. Restart the iPlanet Application Server with the commands:

   ```
   iascontrol stop
   iascontrol kill
   iascontrol start
   ```

7. Check in the logfile **<iASInstallDir>/logs/ias.log** that the application server successfully connected to the master agent. You should see the following line:
   kas> SNMP: Connected to master agent

Starting SNMP Subagents for the iPlanet Web Server

1. Use your Web browser to access the iPlanet Web Server.
2. Choose the Web server you wish to administer, and click the **Manage** button.
3. Select the **Monitor** tab, and click **SNMP Subagent Configuration** on the left side of the page.
4. Type in the configuration information and set the radio button **Enable SNMP Statistics Collection** to **On**.
5. Click **SNMP Subagent Control**.
6. Click the **Start** button.

Starting SNMP Subagents for the iPlanet Directory Server

1. Use the Netscape Administration Console to manage the iPlanet Directory Server.
2. Select the **Configuration** tab.
3. Click the **SNMP** tab in the Configuration frame.
4. Select the **Enable statistics collection** check box.
5. Set "Master Host" to "localhost".
6. Set "Master port" to 199.
7. In the other fields, enter the appropriate information.
8. Click the **Start Subagent** button.

Summary Note

Use your SNMP management tool to query the SNMP master agent on port 161. You should see all the information provided by the Solaris SNMP agent as well as any iPlanet subagents that you have configured.

The next time that you boot Solaris, the Sun and iPlanet SNMP agents will be started automatically by the boot scripts which you have configured.

Adding a Machine to Monitor

In order to monitor the iPlanet (NAS) resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1 Click the iPlanet (NAS) graph in the graph tree, and drag it into the right pane of the Run view.

2 Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The iPlanet (NAS) dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

3 Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

Note: If the iPlanet SNMP agent is running on a different port than the default SNMP port, you must define the port number. Enter the following information in the Add Machine dialog box:
<server name:port number>

For example: digi:8888

In addition, you can define the default port for your iPlanet server in the configuration file, **snmp.cfg**, located in <**LoadRunner root folder**>**dat****monitors**. For example, if the port used by the SNMP agent on your iPlanet server is 8888, you should edit the **snmp.cfg** file as follows:

```
; iPlanet (NAS)
[cm_snmp_mon_nas]
port=8888
```

---

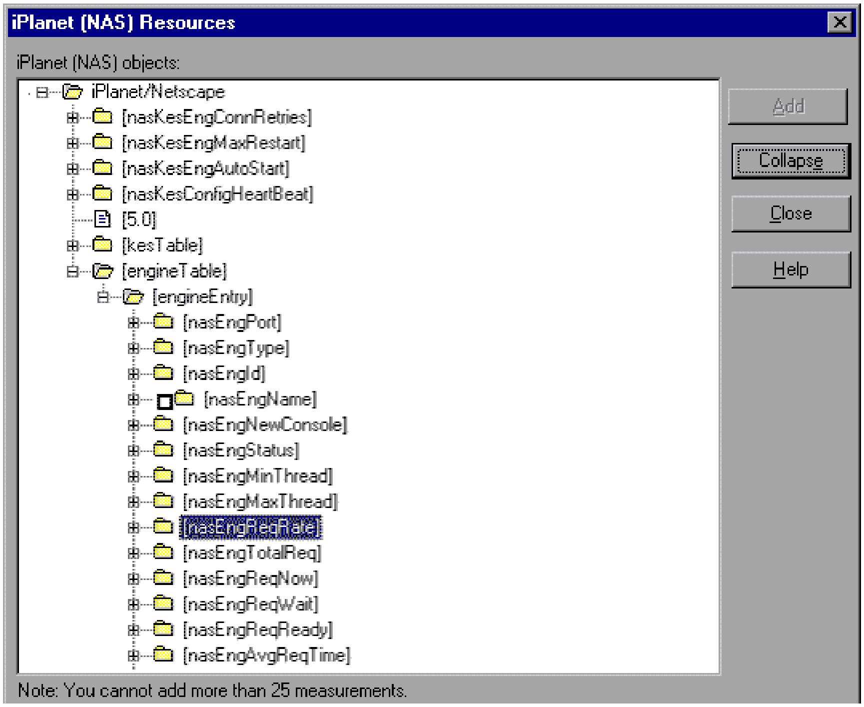
4. In the **Resource Measurements** section of the iPlanet (NAS) dialog box, click **Add**.
5. Continue with “Configuring the iPlanet (NAS) Monitor” on page 172.

Configuring the iPlanet (NAS) Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which objects to monitor on the machine.

To configure the iPlanet (NAS) monitor:

1 When you click **Add** to add a measurement, the iPlanet (NAS) Resources dialog box opens.



2 Browse the iPlanet (NAS) Resources Object tree, and select performance counters, as described in “Understanding the iPlanet (NAS) Resources Dialog Box” on page 174.

For a description of the available measurements, see “iPlanet (NAS) Performance Counters” on page 174.

3 Add all the desired resources to the list, and click **Close**. The resources that you selected appear in the **Resource Measurements on**: *<machine>* section of the iPlanet (NAS) dialog box.

Note: The iPlanet (NAS) monitor can only monitor up to 25 measurements.

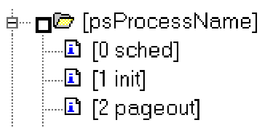
---

4 Click **OK** in the iPlanet (NAS) dialog box to activate the monitor.

Improving the Level of Measurement Information

You can improve the level of measurement information for the iPlanet (NAS) monitor by enabling measurements with string values to be listed (in addition to measurements with numeric values), and by enabling the name modifier (which displays the string value as an identifying part of the measurement name).

In the following example of a measurement using the name modifier, the string value of ProcessName (sched) is displayed in addition to its instance ID (0):



To enable this feature, add the following line to the <**LoadRunner root folder**>**\dat\monitors\snmp.cfg** file:

SNMP_show_string_nodes=1

Usage Notes: You can select more than one name modifier, but the first in the hierarchy will be used. Each time the iPlanet (NAS) Add Measurements dialog box opens, the information is reread from the **snmp.cfg** file. You cannot add the same measurement twice (once with a name modifier and once without it). If you do so, an error message is issued.

Understanding the iPlanet (NAS) Resources Dialog Box

The iPlanet (NAS) dialog box lets you select the iPlanet (NAS) server resources to monitor using the Simple Network Management Protocol (SNMP).

- **iPlanet (NAS) SNMP Objects.** Select each required object and click **Add**. Click **Explain** for the ID number and a description of the selected object.
- **Explain.** Displays a description of the selected object.

Note: The iPlanet (NAS) monitor can only monitor up to 25 measurements.

---

iPlanet (NAS) Performance Counters

The following tables describe the counters that can be monitored:

Netscape Performance Counters

The following counters measure Netscape performance:

Measurement	Description
nasKesEngConn Retries	The maximum number of times the administration server will try to connect to an engine.
nasKesEngMax Restart	The maximum number of times the administration server will restart an engine after a failure.
nasKesEngAutoStart	Start all the engines at startup of the administration server.
nasKesConfigHeart Beat	Heart Beat.

KES Performance Counters

The following counters measure KES performance:

Measurement	Description
nasKesId	The ID of the KES this engine belongs to.
nasKesMinThread	The default minimum number of threads per engine.
nasKesMaxThread	The default maximum number of threads per engine.
nasKesLoadBalancer Disable	Enable or disable the load balancer service.
nasKesCpuLoad	The total CPU usage on this host.
nasKesDiskLoad	The total disk usage on this host.
nasKesMemLoad	The total memory usage on this host.
nasKesRequestLoad	The number of requests on this NAS.
nasKesCpuLoad Factor	The relative importance of CPU usage in computing the server load. This number is specified as a percent. The sum of all server load factors, CPULoad, DiskLoad, MemLoad and ExecReqs must equal 100%.
nasKesDiskLoad Factor	The relative importance of disk usage in computing the server load. This number is specified as a percent. The sum of all server load factors, CPULoad, DiskLoad, MemLoad and ExecReqs must equal 100%.
nasKesMemLoad Factor	The relative importance of memory usage in computing the server load. This number is specified as a percent. The sum of all server load factors, CPULoad, DiskLoad, MemLoad and ExecReqs must equal 100%.
nasKesAppLogics RunningFactor	The relative importance of the number of times an AppLogic is run in computing the AppLogic execution performance. This figure is specified as a percent. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%.

Measurement	Description
nasKesResults CachedFactor	The relative importance of the cached results of an AppLogic in computing the AppLogic execution performance. This figure is specified as a percent. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%
nasKesAvgExecTime Factor	The relative importance of the average execution time of an AppLogic in computing the AppLogic execution performance. This figure is specified as a percent. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%
nasKesLastExec TimeFactor	The relative importance of the last execution time of an AppLogic in computing the AppLogic execution performance. This figure is specified as a percent. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%
nasKesHitsFactor	The relative importance of the number of AppLogics running in computing the AppLogic execution performance. This figure is specified as a percent. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%
nasKesServerLoad Factor	The relative importance of the server load (computed using the four server load factors) in computing AppLogic execution performance. The sum of all agent load factors, ResultCached, AvgExecTime, LastExecTime, and ServerLoad must equal 100%.
nasKesBroadcast Interval	The length of time (in seconds) between each broadcast attempt from the load balancer daemon.
nasKesApplogic BroadcastInterval	The length of time (in seconds) between each broadcast of AppLogic load information across all the servers in the cluster. This should be greater than nasKesBroadcastInterval.

Measurement	Description
nasKesServer BroadcastInterval	The length of time (in seconds) between each broadcast of server load information across all the servers in the cluster. This should be greater than nasKesBroadcastInterval.
nasKesServerLoad UpdateInterval	The length of time (in seconds) between each update of server load information. A server load update applies to the server load data that has been sampled up until the moment when the update occurs.
nasKesCpuLoad UpdateInterval	The length of time (in seconds) between each sampling of CPU usage.
nasKesDiskLoad UpdateInterval	The length of time (in seconds) between each sampling of disk usage.
nasKesMemLoad UpdateInterval	The length of time (in seconds) between each sampling of memory thrashes.
nasKesTotalReqs UpdateInterval	The length of time (in seconds) between each sampling of the number of requests.
nasKesMaxHops	The maximum number of times a request can be loaded.
nasKesODBCReq MinThread	The minimum number of threads reserved to process asynchronous requests.
nasKesODBCReq MaxThread	The maximum number of threads reserved to process asynchronous requests.
nasKesODBCCache MaxConns	The maximum number of connections opened between NAS and the database.
nasKesODBCCache FreeSlots	The minimum number of cached connections established between NAS and the database.
nasKesODBCCache Timeout	The time after which an idle connection is dropped.
nasKesODBCCache Interval	The interval (in seconds) at which the cache cleaner will try to disconnect connections already idle for longer than the specified timeout.
nasKesODBCConn GiveupTime	The maximum amount of time the driver will try to connect to the database.

Measurement	Description
nasKesODBCCache Debug	Turns on the connection cache debug information.
nasKesODBCResult SetInitRows	The number of rows fetched at once from the database.
nasKesODBCResult SetMaxRows	The maximum number of rows the cached result set can contain.
nasKesODBCResult SetMaxSize	The maximum size of result set the driver will cache.
nasKesODBCSql Debug	Turns on SQL debug information.
nasKesODBCEnable Parser	Turns on SQL parsing.
nasKesORCLReqMin Thread	The minimum number of threads reserved to process asynchronous requests.
nasKesORCLReq MaxThread	The maximum number of threads reserved to process asynchronous requests.
nasKesORCLCache MaxConns	The maximum number of connections opened between NAS and the database.
nasKesORCLCache FreeSlots	The minimum number of cached connections established between NAS and the database.
nasKesORCLCache Timeout	The time after which an idle connection is dropped.
nasKesORCLCache Interval	The interval (in seconds) at which the cache cleaner will try to disconnect connections already idle for longer than the specified timeout.
nasKesORCLConn GiveupTime	The maximum amount of time the driver will spend trying to obtain a connection to Oracle.
nasKesORCLCache Debug	Turns on the connection cache debug information.
nasKesORCLResult SetInitRows	The number of rows fetched at once from the database.

Measurement	Description
nasKesORCLResult SetMaxRows	The maximum number of rows the cached result set can contain.
nasKesORCLResult SetMaxSize	The maximum size of result set the driver will cache.
nasKesORCLSql Debug	Turns on sql debug information.
nasKesSYBReqMin Thread	The minimum number of threads reserved to process asynchronous requests.
nasKesSYBReqMax Thread	The maximum number of threads reserved to process asynchronous request.
nasKesSYBCache MaxConns	The maximum number of connections opened between NAS and the database.
nasKesSYBCache FreeSlots	The minimum number of cached connections established between NAS and the database.
nasKesSYBCache Timeout	The time after which an idle connection is dropped.
nasKesSYBCache Interval	The interval (in seconds) at which the cache cleaner will try to disconnect connections already idle for longer than the specified timeout.
nasKesSYBConn GiveupTime	The maximum time the driver will spend trying to obtain a connection to Sybase before giving up.
nasKesSYBCache Debug	Turns on the connection cache debug information.
nasKesSYBResultSet InitRows	The number of rows fetched at once from the database.
nasKesSYBResultSet MaxRows	The maximum number of rows the cached result set can contain.
nasKesSYBResultSet MaxSize	The maximum size of result set the driver will cache.

Engine Performance Counters

The following counters measure Engine performance:

Measurement	Description
nasEngKesPort	The port of the KXS this engine serves. This is supplied as part of the object ID and cannot be modified after creation.
nasEngPort	The TCP/IP port this engine is listening on. The port can only be specified at the creation of the engine. It is not allowed to modify it.
nasEngType	Type of the engine: executive(0), Java(1000), C++(3000).
nasEngId	The ID is an incremental number starting at 0. The ID cannot be modified.
nasEngName	The name of this engine. This is an informational string that contains kcs, kxs or kjs.
nasEngNewConsole	Starts each engine in a new console window.
nasEngStatus	The status column used to add, remove, enable or disable an engine. To create an engine, one needs to set. This follows rfc1443.
nasEngMinThread	The default minimum number of threads per engine.
nasEngMaxThread	The default maximum number of threads per engine.
nasEngReqRate	The rate at which requests arrive.
nasEngTotalReq	The total number of requests processed since engine startup.
nasEngReqNow	The number of requests being processed.
nasEngReqWait	The requests waiting to be serviced.
nasEngReqReady	The requests that are ready to be serviced.
nasEngAvgReqTime	The average request processing time.
nasEngThreadNow	Number of threads in use by the request manager.
nasEngThreadWait	The number of idle threads.

Measurement	Description
nasEngWebReq Queue	The number of web requests that are queued.
nasEngFailedReq	The number of requests that failed.
nasEngTotalConn	The total number of connections opened.
nasEngTotalConn Now	The total number of connections in use.
nasEngTotalAccept	The total number of connections listening to incoming requests.
nasEngTotalAccept Now	The total number of connections listening to incoming connections in use.
nasEngTotalSent	The total number of packets sent.
nasEngTotalSentBytes	The total number of bytes sent.
nasEngTotalRecv	The total number of packets received.
nasEngTotalRecvBytes	The total number of bytes received.
nasEngBindTotal	The number of AppLogic bound since startup.
nasEngBindTotal Cached	The number of AppLogic cached since startup.
nasEngTotalThreads	Total number of threads created in this process.
nasEngCurrent Threads	Total number of threads in use in this process.
nasEngSleeping Threads	Number of threads sleeping in this process.
nasEngDAETotal Query	Total number of queries executed since startup.
nasEngDAEQuery Now	The number of queries being processed.
nasEngDAETotal Conn	The number of logical connections created since startup.

Measurement	Description
nasEngDAEConn Now	The number of logical connections in use.
nasEngDAECache Count	The number of caches.
nasEngODBCQuery Total	Total number of queries executed since startup.
nasEngODBC PreparedQueryTotal	Total number of ODBC prepared queries executed since startup.
nasEngODBCConn Total	Total number of connections opened since startup.
nasEngODBCConn Now	Number of connections currently opened.
nasEngORCLQuery Total	Total number of queries executed since startup.
nasEngORCL PreparedQueryTotal	Total number of prepared queries executed since startup.
nasEngORCLConn Total	Total number of connections established with Oracle since startup.
nasEngORCLConn Now	Number of connections opened with Oracle now.
nasEngSYBQuery Total	Total number of queries the driver processed since startup.
nasEngSYBPreparedQ ueryTotal	Total number of prepared queries processed since startup.
nasEngSYBConnTotal	Total number of connections opened since startup.
nasEngSYBConnNow	Number of SYB connections opened now.
nasStatusTrapEntry	The KES definition.
nasTrapKesIpAddress	The IP Address of KES host.
nasTrapKesPort	The port of the main engine of this NAS.

Measurement	Description
nasTrapEngPort	The port of the engine generating this event.
nasTrapEngState	The port of the engine generating this event.

20

Microsoft Active Server Pages Monitoring

The Microsoft Active Server Pages (ASP) monitor displays statistics about the resource usage on the ASP server during the scenario run.

To obtain data for this graph, you need to configure the Microsoft ASP online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You select measurements to monitor the Microsoft ASP application server using the MS Active Server Pages dialog box.

Note: To monitor an ASP server through a firewall, use TCP, port 139.

This chapter includes:

Adding a Machine to Monitor

In order to monitor the MS Active Server resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the MS Active Server Pages graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The MS Active Server Pages dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.
4. In the **Resource Measurements** section of the MS Active Server Pages dialog box, select the default measurements you want to monitor.

   For a description of the available measurements, see "MS Active Server Pages Performance Counters" on page 188.

   Note: To change the default counters for the Microsoft ASP monitor, see "Changing a Monitor's Default Counters" on page 395.

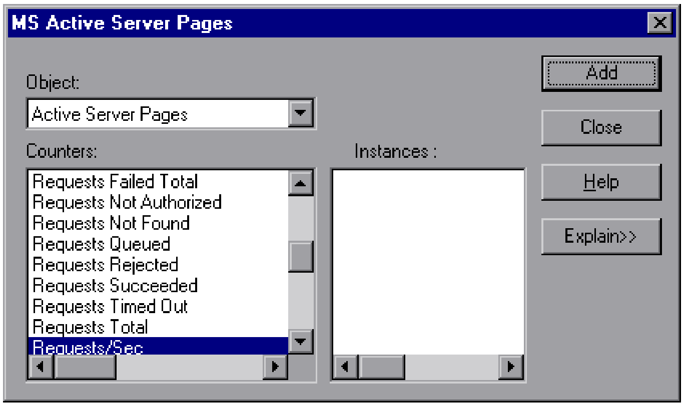
   ---
5. To select additional measurements, click **Add** in the **Resource Measurements** section.
6. Continue with Configuring the Microsoft Active Server Pages Monitor below.

Configuring the Microsoft Active Server Pages Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the MS Active Server Pages monitor:

1 When you click **Add** to add a measurement, the MS Active Server Pages dialog box opens displaying the Active Server Pages object, its counters, and instances.



For each measurement, select an object, counter, and instance, and then click **Add**, as described in "Understanding the Microsoft Active Server Pages Dialog Box" on page 188.

For a description of the available measurements, see "MS Active Server Pages Performance Counters" on page 188.

Note: To change the default counters for the Microsoft ASP monitor, see "Changing a Monitor's Default Counters" on page 395.

---

2 Add all the desired resources to the list, and click **Close**. The counters that you selected appear in the **Resource Measurements on**: <*machine*> section of the MS Active Server Pages dialog box.

3 Click **OK** in the MS Active Server Pages dialog box to activate the monitor.

Understanding the Microsoft Active Server Pages Dialog Box

The MS Active Server Pages dialog box lets you select the items to monitor on the MS Active Server Pages application server.

- **Object.** Select the object being monitored on the specified machine.
- **Counters.** Select a resource counter to monitor. Select multiple counters using the CTRL key. For an explanation of each counter, click **Explain**.
- **Instances.** If multiple instances of the selected counter are running, select one or more instances to monitor for the selected counter.
- **Explain.** Displays a description of the selected counter.

MS Active Server Pages Performance Counters

The following table describes the default counters that can be monitored:

Measurement	Description
Errors per Second	The number of errors per second.
Requests Wait Time	The number of milliseconds the most recent request was waiting in the queue.
Requests Executing	The number of requests currently executing.
Requests Queued	The number of requests waiting in the queue for service.
Requests Rejected	The total number of requests not executed because there were insufficient resources to process them.
Requests Not Found	The number of requests for files that were not found.
Requests/sec	The number of requests executed per second.
Memory Allocated	The total amount of memory, in bytes, currently allocated by Active Server Pages.
Errors During Script Run-Time	The number of failed requests due to run-time errors.

Measurement	Description
Sessions Current	The current number of sessions being serviced.
Transactions/sec	The number of transactions started per second.

21

WebLogic (SNMP) Monitoring

The WebLogic (SNMP) monitor displays statistics about the resource usage on the WebLogic (SNMP) server (version 6.0 and earlier) during the scenario run. The WebLogic (SNMP) monitor uses SNMP to retrieve server statistics.

This chapter includes:

To use this monitor, you must make sure that a version prior to WebLogic 6.0 is installed on your server, and that the SNMP agent is installed and activated on the server.

For instructions on installing the SNMP agent, see http://edocs.bea.com/wls/docs51/admindocs/snmpagent.html.

To obtain data for this graph, you need to configure the WebLogic (SNMP) online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

Note: To monitor a WebLogic (SNMP) server, use port 161 or 162, depending on the configuration of the agent.

Adding a Machine to Monitor

In order to monitor the WebLogic (SNMP) resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the WebLogic (SNMP) graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The WebLogic (SNMP) dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

Note: If the WebLogic SNMP agent is running on a different port than the default SNMP port, you must define the port number. Enter the following information in the Add Machine dialog box:
<server name:port number>

For example: digi:8888

In addition, you can define the default port for your WebLogic server in the configuration file, **snmp.cfg**, located in **<LoadRunner root folder>\dat\monitors**. For example, if the port used by the SNMP agent on your WebLogic server is 8888, you should edit the **snmp.cfg** file as follows:

```
; WebLogic
[cm_snmp_mon_isp]
port=8888
```

---

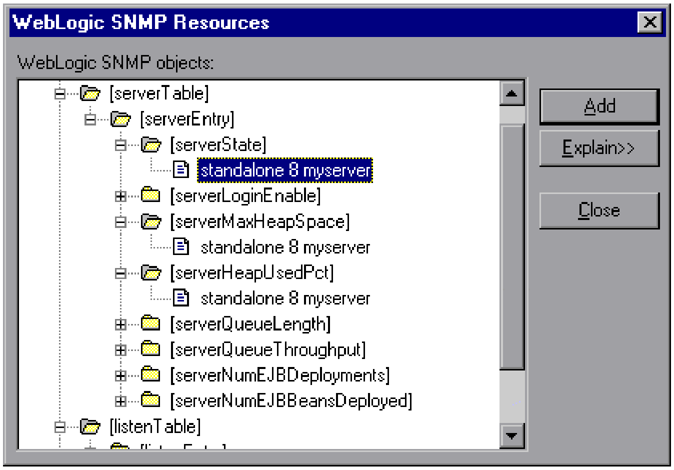
4. In the **Resource Measurements** section of the WebLogic (SNMP) dialog box, click **Add**.
5. Continue with “Configuring the WebLogic (SNMP) Monitor” on page 193.

Configuring the WebLogic (SNMP) Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the WebLogic (SNMP) monitor:

1 When you click **Add** to add a measurement, the WebLogic SNMP Resources dialog box opens, displaying the available measurements.



2 Browse the WebLogic SNMP Objects tree, and select performance counters, as described in “Understanding the WebLogic (SNMP) Resources Dialog Box” on page 194.

For a description of the available measurements, see “WebLogic (SNMP) Performance Counters” on page 195.

Note: The WebLogic (SNMP) monitor can only monitor up to 25 measurements.

---

3 After selecting and adding the required objects, click **Close**.

4 Click **OK** in the WebLogic (SNMP) dialog box to activate the monitor.

Understanding the WebLogic (SNMP) Resources Dialog Box

The WebLogic (SNMP) dialog box lets you select the items to monitor on the WebLogic (SNMP) application server. To use this monitor, you must make sure that a version prior to WebLogic 6.0 is installed on your server, and that the SNMP agent is installed and activated on the server. For instructions on installing the SNMP agent, see http://edocs.bea.com/wls/docs51/admindocs/snmpagent.html.

- **WebLogic SNMP Objects.** Select each required object and click **Add** (you can select only one object at a time). Click **Explain** for a description of the selected object.
- **Explain.** Displays a description of the selected object.

Note: The WebLogic (SNMP) monitor can only monitor up to 25 measurements.

WebLogic (SNMP) Performance Counters

The following tables describe the measurements and server properties that can be monitored.

Server Table

The Server Table lists all WebLogic (SNMP) servers that are being monitored by the agent. A server must be contacted or be reported as a member of a cluster at least once before it will appear in this table. Servers are only reported as a member of a cluster when they are actively participating in the cluster, or shortly thereafter.

Measurement	Description
ServerState	The state of the WebLogic server, as inferred by the SNMP agent. **Up** implies that the agent can contact the server. **Down** implies that the agent cannot contact the server.
ServerLoginEnable	This value is true if client logins are enabled on the server.
ServerMaxHeapSpace	The maximum heap size for this server, in KB
ServerHeapUsedPct	The percentage of heap space currently in use on the server
ServerQueueLength	The current length of the server execute queue
ServerQueueThroughput	The current throughput of execute queue, expressed as the number of requests processed per second
ServerNumEJBDeployment	The total number of EJB deployment units known to the server
ServerNumEJBBeansDeployed	The total number of EJB beans actively deployed on the server

Listen Table

The Listen Table is the set of protocols, IP addresses, and port combinations on which servers are listening. There will be multiple entries for each server: one for each protocol, ipAddr, port combination. If clustering is used, the clustering-related MIB objects will assume a higher priority.

Measurement	Description
ListenPort	Port number.
ListenAdminOK	**True** if admin requests are allowed on this (protocol, ipAddr, port) combination; otherwise false.
ListenState	**Listening** if the (protocol, ipAddr, port) combination is enabled on the server; **Not Listening** if it is not. The server may be listening but not accepting new clients if its server Login Enable state is false. In this case, existing clients will continue to function, but new ones will not.

ClassPath Table

The ClassPath Table is the table of classpath elements for Java, WebLogic (SNMP) servers, and servlets. There are multiple entries in this table for each server. There may also be multiple entries for each path on a server. If clustering is used, the clustering-related MIB objects will assume a higher priority.

Measurement	Description
CPType	The type of CP element: Java, WebLogic, servlet. A Java CPType means the CP element is one of the elements in the normal Java classpath. A WebLogic CPType means the CP element is one of the elements in weblogic.class.path. A servlet CPType means the CP element is one of the elements in the dynamic servlet classpath.
CPIndex	The position of an element within its path. The index starts at 1.

22

WebSphere Application Server Monitoring

The WebSphere Application Server Monitor allows you to monitor the availability and server statistics of a IBM WebSphere Application Server 3.5.x, 4.x, and 5.x. The error and warning thresholds for the monitor can be set on as many as ten WebSphere Application Server performance statistics.

The WebSphere Application Server Monitor monitors the server performance statistics from IBM WebSphere servers using the performance monitoring interfaces provided with WebSphere. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Application Server Monitor instance for each WebSphere Application Server in your environment.

To obtain data for this graph, you need to configure the WebSphere Application Server online monitor (from the Controller) and select the measurements you want to display before running the scenario.

This chapter includes:

Setting up the Monitoring Environment

Before you can use the WebSphere Application Server monitor, you need to configure the server environment.

Ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.

For WebSphere 3.5.x and 4.x

- You must first install the IBM WebSphere Administrator's Console on the SiteScope server if you are monitoring WebSphere versions 3.5.x or 4.x. When installing the Administrator's Console:
  - Select the **Custom** installation option.
  - In the Choose Application Server Components dialog box, select **Administrator's Console** and **IBM JDK 1.2.2**.
  - You will need to specify the machine you want to monitor during the installation.
- You must enable the WebSphere servers to be monitored.
  - For WebSphere 3.5.x, enable EPM Counters on the WebSphere server.
  - For WebSphere 4.x and 5.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server.

You enable the counters for the application you want to monitor via the WebSphere Administrator's Console.

For WebSphere 4.x:

- When you have selected resources to monitor, select the **Performance** option.
- In the dialog box that opens, expand the **Performance Modules** tree. In order to manage different levels of performance data, select the performance modules and choose a performance level, and click **Set**.

- Alternatively, on WebSphere 3.5.x, you can set the EPM Specification to:

  ```
  epm=high:epm.beanMethodData=none
  ```

  through the WebSphere Administrator's Console.
- If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

For WebSphere 5.x

In the server environment:

1. Select **Servers** > **Application Servers**, and select the server to be monitored from the Application Server list.
2. In the Configuration tab's **Additional Properties** list, click **Performance Monitoring Service**.
3. Select the **Start Up** check box.
4. In the **Initial specification level** section select **Standard** or **Custom**.
5. Click **Apply**.

To monitor WebSphere version 5.x, the necessary WebSphere libraries must be available on the SiteScope server. This means that a WebSphere 5.x client must be installed on the SiteScope server.

To install the correct client software on a SiteScope server:

1. When installing WebSphere 5.x, select the following options from the Custom Options menu:
   - Administration and Administrative Console
   - Performance and Analysis Tools

Note: Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the Sitescope WebSphere Application Server monitor. The SiteScope monitor will only work when a complete WebSphere production installation is available.

---

2 Copy all of the files from the *<WebSphere 5.x Application Server installation>***lib** folder to the *<client installation>***lib** folder (see step 1 above).

3 The WebSphere 5.x server and client settings have to match. This means that the SiteScope WebSphere Application Server Monitor will not be able to monitor a WebSphere 5.1 application server if the client libraries are from a WebSphere 5.0 application server, and vice versa.

Client libraries should be installed in separate folders with clearly distinct directory names, such as WebSphere50 and WebSphere51, to avoid confusion and SiteScope setup errors.

4 The **sas.props** file should be replaced with **soap.props** for WebSphere 5.x installations.

Note: The WebSphere 5.x SiteScope monitor uses the WebSphere JMX interface, so the port number used to communicate with the application server is the SOAP port number. By default, the SOAP port number is **8880**.

---

5 If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

General information

If security has been enabled on the WebSphere server, you must copy the security keyring from the WebSphere server to SiteScope. A keyring is a certification used by the server to identify the client.

Adding a Machine to Monitor

In order to monitor the WebSphere Application Server of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller

1. Click the **WebSphere Application Server** graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The WebSphere Application Server dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs, and click **OK**.

   In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.
4. In the **Resource Measurements** section of the WebSphere Application Server dialog box, click **Add**.
5. Continue with "Configuring the WebSphere Application Server Monitor" on page 204.

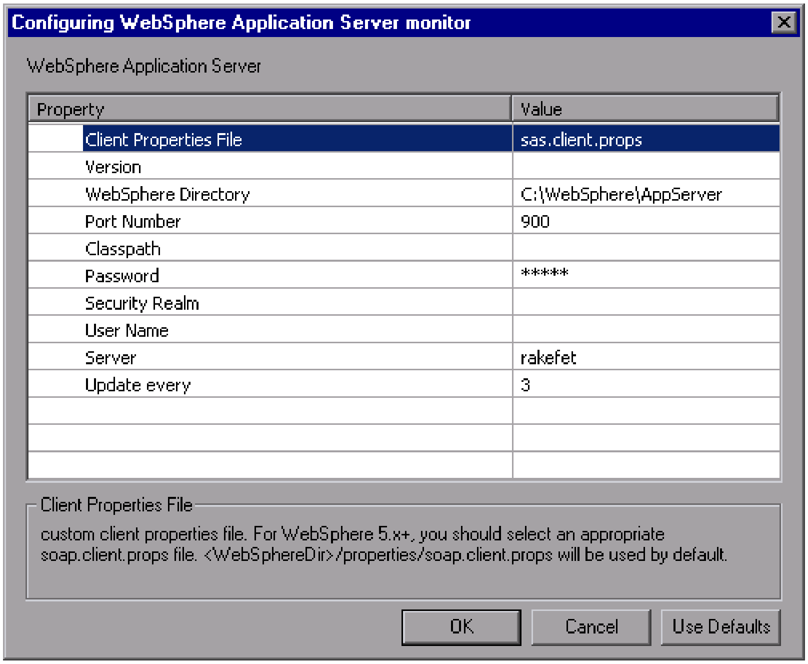
Configuring the WebSphere Application Server Monitor

After you have added the machine that you are monitoring, you need to configure the monitor and choose which measurements to monitor.

To configure the WebSphere Application Server monitor:

1 The first time you add a measurement to the monitor, you need to configure the monitor properties. When you click **Add** to add a measurement, the Configuring WebSphere Application Server Monitor dialog box opens.

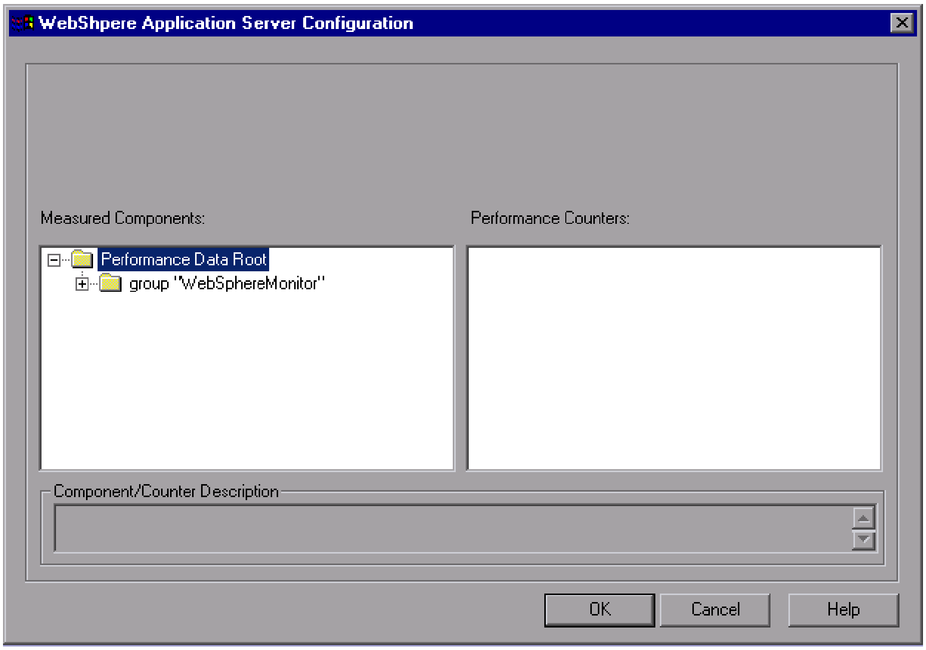
2 Enter values for the monitor properties as described in "Understanding the Configuring WebSphere Application Server Monitor Dialog Box" on page 206, and click **OK**.



3 The WebSphere Application Server Configuration dialog box opens.

Browse the **Measured Components** tree and select the performance counters on the right, as described in "Understanding the WebSphere Application Server Configuration Dialog Box" on page 207.

Click a component or counter to see its description in the **Component/Counter Description** section.



4 Click **OK** to close the WebSphere Application Server Configuration dialog box. The counters that you selected appear in the **Resource Measurements on**: <*machine*> section of the WebSphere Application Server dialog box.

5 Click **OK** in the WebSphere Application Server dialog box to activate the WebSphere Application Server monitor.

Understanding the Configuring WebSphere Application Server Monitor Dialog Box

You configure the WebSphere Application Server monitor in the Configuring WebSphere Application Server Monitor dialog box.

- **Client Properties File.** Enter the custom client properties file. Select an appropriate soap.client.props file. By default, the **<WebSphere>/properties/soap.client.props** file is used.
- **Version.** Enter the version of the WebSphere server.
- **WebSphere Directory.** Enter the path to the WebSphere directory. This directory should contain at least an Admin Console installation.
- **Port Number.** Enter the port number of WebSphere server. This should be the SOAP port for WebSphere 5.x+. The default port number is 8880.
- **Classpath.** Enter any extra classpath elements needed for the monitor program.
- **Password.** Enter the password that SiteScope should use to log on to WebSphere server.
- **Security Realm.** Enter the security realm for the WebSphere server (3.5x only).
- **User Name.** Enter the user name that SiteScope should use to log on to WebSphere server.
- **Server.** Enter the name of the server where the WebSphere application is running. Do not enter backslashes (\\) that indicate a UNC path as part of the name of the server.
- **Update every.** The number entered here indicates the amount of time, in seconds, between one monitor check and the next. By default the monitor updates every 3 seconds.

Understanding the WebSphere Application Server Configuration Dialog Box

The WebSphere Application Server Configuration dialog box enables you to select the performance counters to monitor using the WebSphere application server.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

WebSphere Application Server Performance Counters

There is a large number of counters available for the WebSphere Application Server monitor. The list of available counters will vary depending on which version of WebSphere you are running.

The list of available counters may include the following:

Run-Time Resources

These are resources related to the Java Virtual Machine run time, as well as the ORB.

Measurement	Description
MemoryFree	The amount of free memory remaining in the Java Virtual Machine.
MemoryTotal	The total memory allocated for the Java Virtual Machine.
MemoryUse	The total memory in use on the Java Virtual Machine.

BeanData

Every home on the server provides performance data, depending on the type of bean deployed in the home. The top level bean data holds an aggregate of all the containers.

Measurement	Description
BeanDestroys	The number of times an individual bean object was destroyed. This applies to any bean, regardless of its type.
StatelessBeanDestroys	The number of times a stateless session bean object was destroyed.
StatefulBeanDestroys	The number of times a stateful session bean object was destroyed.

BeanObjectPool

The server holds a cache of bean objects. Each home has a cache and there is therefore one BeanObjectPoolContainer per container. The top level, BeanObjectPool, holds an aggregate of all the containers data.

Measurement	Description
NumGetFound	The number of calls to the pool that resulted in finding an available bean.
NumPutsDiscarded	The number of times releasing a bean to the pool resulted in the bean being discarded because the pool was full.

OrbThreadPool

These are resources related to the ORB thread pool that is on the server.

Measurement	Description
ActiveThreads	The average number of active threads in the pool.
TotalThreads	The average number of threads in the pool.
PercentTimeMaxed	The average percent of the time that the number of threads in the pool reached or exceeded the desired maximum number.

DBConnectionMgr

These are resources related to the database connection manager. The manager consists of a series of data sources, as well as a top-level aggregate of each of the performance metrics.

Measurement	Description
ConnectionWaitTime	The average time (in seconds) of a connection grant.
ConnectionTime	The average time (in seconds) that a connection is in use.
ConnectionPercentUsed	The average percentage of the pool that is in use.

TransactionData

These are resources that pertain to transactions.

Measurement	Description
NumTransactions	The number of transactions processed.
ActiveTransactions	The average number of active transactions.
TransactionRT	The average duration of each transaction.
RolledBack	The number of transactions rolled back.
Timeouts	The number of transactions that timed out due to inactivity timeouts.
TransactionSuspended	The average number of times that a transaction was suspended.

ServletEngine

These are resources that are related to servlets and JSPs.

Measurement	Description
ServletErrors	The number of requests that resulted in an error or an exception.

Sessions

These are general metrics regarding the HTTP session pool.

Measurement	Description
SessionsInvalidated	The number of invalidated sessions. May not be valid when using sessions in the database mode.

Part IX

Database Server Resource Monitoring

23

Introduction to Database Resource Monitoring

You monitor DB2, Oracle, SQL Server, or Sybase database resource usage during a scenario run using LoadRunner's Database Server Resource monitors.

The DB2, Oracle, SQL Server, or Sybase database server resource monitors measure statistics for DB2, Oracle, SQL Server, or Sybase database servers. During a scenario run, you use these monitors to isolate database server performance bottlenecks.

For each database server, you configure the measurements you want to monitor before running your scenario. To run the DB2, Oracle, and Sybase monitors, you must also install the client libraries on the database server you want to monitor.

24

DB2 Monitoring

The DB2 monitor shows the resource usage on the DB2 database server machine.

To monitor the DB2 database server machine, you must first set up the DB2 monitor environment. You then enable the DB2 monitor (from the Controller) by selecting the counters you want the monitor to measure. You select these counters using the DB2 Monitor Configuration dialog box.

Note: If there is no application working with a database, you can only monitor the database manager instance.

This chapter includes:

Setting Up the Monitoring Environment

Before monitoring a DB2 database server, you must set up the monitor environment.

To set up the DB2 monitor environment:

1. Install all the client files and libraries on the Controller machine.
2. Select **Start** > **Programs** > **DB2 for Windows NT** > **Control Center**. Enter your DB2 server username and password (with administrative privileges).
3. In the console that opens, right-click **Systems**, and select **Add**.
4. Enter the following settings in the dialog box:
   - **System Name**. <server name>
   - **Remote Instance**. DB2
   - **Host Name**. <server name>
   - **Service Name**. The DB2 server port. The default value is 50000.
5. Click **Retrieve**, and then **OK**.

Note: If you receive an error message after clicking **Retrieve**, repeat steps 3 and 4, and click **OK**.

---

6. Expand the <server name> node in the console tree.
7. Right-click **Instance**, and select **Add**.
8. Enter the following settings in the dialog box:
   - **Remote Instance.** DB2
   - **Instance Name.** the database instance to be called from the Controller
   - **Host Name.** <server name>
   - **Service Name.** The DB2 server port. The default value is 50000.

9 Click **OK** and close the Control Center.

Note: You can only work with a single Database Manager instance during each monitoring session.

Adding a Machine to Monitor

In order to monitor the DB2 resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

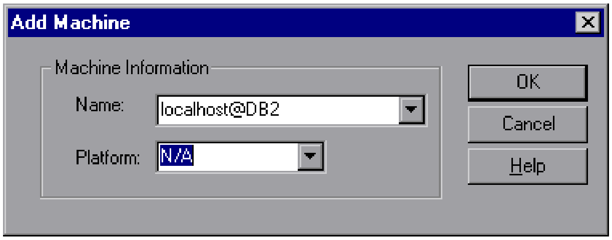
To add a machine to the Controller:

1 Click the DB2 graph in the graph tree, and drag it into the right pane of the Run view.

2 Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The DB2 dialog box opens.

In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

3 Enter the DB2 server machine name followed by the @ sign and the database instance you specified in the DB2 Control Center. In the Platform box, select **N/A**.



Click **OK** to save the information you entered and close the dialog box.

4 In the **Resource Measurements** section of the DB2 dialog box, click **Add**.

5 Continue with Configuring the DB2 Monitor below.

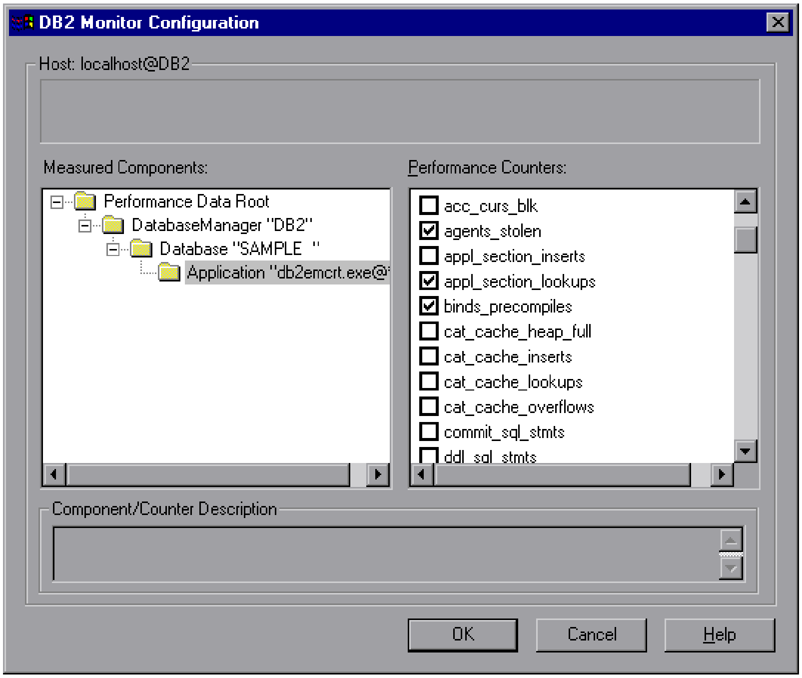
Configuring the DB2 Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the DB2 monitor:

1 When you click **Add** to add a measurement, a dialog box opens requesting your DB2 Server username and password. Enter the details and click **OK**.

2 The DB2 Monitor Configuration dialog box opens, displaying the available measurements.



Browse the Measured Components tree, and select performance counters, as described in "Understanding the DB2 Monitor Configuration Dialog Box" on page 220, and then click **OK**.

For a description of the available measurements, see "DB2 Performance Counters" on page 221.

3 Click **OK**. The measurements that you selected appear in the **Resource Measurements on:** <*machine*> section of the DB2 dialog box.

4 Click **OK** in the DB2 dialog box to activate the monitor.

Understanding the DB2 Monitor Configuration Dialog Box

The DB2 Monitor Configuration dialog box lets you select the measurements to monitor the resource usage on a DB2 database during a scenario run.

Note: If there is no application working with a database, you can only monitor the database manager instance.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

DB2 Performance Counters

The following tables describe the default counters that can be monitored.

DatabaseManager

The following table lists the DatabaseManager counters:

Measurement	Description
rem_cons_in	The current number of connections initiated from remote clients to the instance of the database manager that is being monitored.
rem_cons_in_exec	The number of remote applications that are currently connected to a database and are currently processing a unit of work within the database manager instance being monitored.
local_cons	The number of local applications that are currently connected to a database within the database manager instance being monitored.
local_cons_in_exec	The number of local applications that are currently connected to a database within the database manager instance being monitored and are currently processing a unit of work.
con_local_dbases	The number of local databases that have applications connected.
agents_registered	The number of agents registered in the database manager instance that is being monitored (coordinator agents and subagents).
agents_waiting_on_token	The number of agents waiting for a token so they can execute a transaction in the database manager.
idle_agents	The number of agents in the agent pool that are currently unassigned to an application and are therefore "idle".
agents_from_pool	The number of agents assigned from the agent pool.

Measurement	Description
agents_created_empty_pool	The number of agents created because the agent pool was empty.
agents_stolen	The number of times that agents are stolen from an application. Agents are stolen when an idle agent associated with an application is reassigned to work on a different application.
comm_private_mem	The amount of private memory that the instance of the database manager has currently committed at the time of the snapshot.
inactive_gw_agents	The number of DRDA agents in the DRDA connections pool that are primed with a connection to a DRDA database, but are inactive.
num_gw_conn_switches	The number of times that an agent from the agents pool was primed with a connection and was stolen for use with a different DRDA database.
sort_heap_allocated	The total number of allocated pages of sort heap space for all sorts at the level chosen and at the time the snapshot was taken.
post_threshold_sorts	The number of sorts that have requested heaps after the sort heap threshold has been reached.
piped_sorts_requested	The number of piped sorts that have been requested.
piped_sorts_accepted	The number of piped sorts that have been accepted.

Database

The following table lists the Database counters:

Measurement	Description
appls_cur_cons	Indicates the number of applications that are currently connected to the database.
appls_in_db2	Indicates the number of applications that are currently connected to the database, and for which the database manager is currently processing a request.
total_sec_cons	The number of connections made by a sub-agent to the database at the node.
num_assoc_agents	At the application level, this is the number of sub-agents associated with an application. At the database level, it is the number of sub-agents for all applications.
sort_heap_allocated	The total number of allocated pages of sort heap space for all sorts at the level chosen and at the time the snapshot was taken.
total_sorts	The total number of sorts that have been executed.
total_sort_time	The total elapsed time (in milliseconds) for all sorts that have been executed.
sort_overflows	The total number of sorts that ran out of sort heap and may have required disk space for temporary storage.
active_sorts	The number of sorts in the database that currently have a sort heap allocated.
total_hash_joins	The total number of hash joins executed.
total_hash_loops	The total number of times that a single partition of a hash join was larger than the available sort heap space.
hash_join_overflows	The number of times that hash join data exceeded the available sort heap space.

Measurement	Description
hash_join_small_overflows	The number of times that hash join data exceeded the available sort heap space by less than 10%.
pool_data_l_reads	Indicates the number of logical read requests for data pages that have gone through the buffer pool.
pool_data_p_reads	The number of read requests that required I/O to get data pages into the buffer pool.
pool_data_writes	Indicates the number of times a buffer pool data page was physically written to disk.
pool_index_l_reads	Indicates the number of logical read requests for index pages that have gone through the buffer pool.
pool_index_p_reads	Indicates the number of physical read requests to get index pages into the buffer pool.
pool_index_writes	Indicates the number of times a buffer pool index page was physically written to disk.
pool_read_time	Provides the total amount of elapsed time spent processing read requests that caused data or index pages to be physically read from disk to buffer pool.
pool_write_time	Provides the total amount of time spent physically writing data or index pages from the buffer pool to disk.
files_closed	The total number of database files closed.
pool_async_data_reads	The number of pages read asynchronously into the buffer pool.
pool_async_data_writes	The number of times a buffer pool data page was physically written to disk by either an asynchronous page cleaner, or a pre-fetcher. A pre-fetcher may have written dirty pages to disk to make space for the pages being pre-fetched.

Measurement	Description
pool_async_index_writes	The number of times a buffer pool index page was physically written to disk by either an asynchronous page cleaner, or a pre-fetcher. A pre-fetcher may have written dirty pages to disk to make space for the pages being pre-fetched.
pool_async_index_reads	The number of index pages read asynchronously into the buffer pool by a pre-fetcher.
pool_async_read_time	The total elapsed time spent reading by database manager pre-fetchers.
pool_async_write_time	The total elapsed time spent writing data or index pages from the buffer pool to disk by database manager page cleaners.
pool_async_data_read_reqs	The number of asynchronous read requests.
pool_lsn_gap_clns	The number of times a page cleaner was invoked because the logging space used had reached a pre-defined criterion for the database.
pool_drty_pg_steal_clns	The number of times a page cleaner was invoked because a synchronous write was needed during the victim buffer replacement for the database.
pool_drty_pg_thrsh_clns	The number of times a page cleaner was invoked because a buffer pool had reached the dirty page threshold criterion for the database.
prefetch_wait_time	The time an application spent waiting for an I/O server (pre-fetcher) to finish loading pages into the buffer pool.
pool_data_to_estore	The number of buffer pool data pages copied to extended storage.
pool_index_to_estore	The number of buffer pool index pages copied to extended storage.
pool_data_from_estore	The number of buffer pool data pages copied from extended storage.
pool_index_from_estore	The number of buffer pool index pages copied from extended storage.

Measurement	Description
direct_reads	The number of read operations that do not use the buffer pool.
direct_writes	The number of write operations that do not use the buffer pool.
direct_read_reqs	The number of requests to perform a direct read of one or more sectors of data.
direct_write_reqs	The number of requests to perform a direct write of one or more sectors of data.
direct_read_time	The elapsed time (in milliseconds) required to perform the direct reads.
direct_write_time	The elapsed time (in milliseconds) required to perform the direct writes.
cat_cache_lookups	The number of times that the catalog cache was referenced to obtain table descriptor information.
cat_cache_inserts	The number of times that the system tried to insert table descriptor information into the catalog cache.
cat_cache_overflows	The number of times that an insert into the catalog cache failed due the catalog cache being full.
cat_cache_heap_full	The number of times that an insert into the catalog cache failed due to a heap-full condition in the database heap.
pkg_cache_lookups	The number of times that an application looked for a section or package in the package cache. At a database level, it indicates the overall number of references since the database was started, or monitor data was reset.
pkg_cache_inserts	The total number of times that a requested section was not available for use and had to be loaded into the package cache. This count includes any implicit prepares performed by the system.

Measurement	Description
pkg_cache_num_overflows	The number of times that the package cache overflowed the bounds of its allocated memory.
appl_section_lookups	Lookups of SQL sections by an application from its SQL work area.
appl_section_inserts	Inserts of SQL sections by an application from its SQL work area.
sec_logs_allocated	The total number of secondary log files that are currently being used for the database.
log_reads	The number of log pages read from disk by the logger.
log_writes	The number of log pages written to disk by the logger.
total_log_used	The total amount of active log space currently used (in bytes) in the database.
locks_held	The number of locks currently held.
lock_list_in_use	The total amount of lock list memory (in bytes) that is in use.
deadlocks	The total number of deadlocks that have occurred.
lock_escals	The number of times that locks have been escalated from several row locks to a table lock.
x_lock_escals	The number of times that locks have been escalated from several row locks to one exclusive table lock, or the number of times an exclusive lock on a row caused the table lock to become an exclusive lock.
lock_timeouts	The number of times that a request to lock an object timed-out instead of being granted.
lock_waits	The total number of times that applications or connections waited for locks.
lock_wait_time	The total elapsed time waited for a lock.

Measurement	Description
locks_waiting	Indicates the number of agents waiting on a lock.
rows_deleted	The number of row deletions attempted.
rows_inserted	The number of row insertions attempted.
rows_updated	The number of row updates attempted.
rows_selected	The number of rows that have been selected and returned to the application.
int_rows_deleted	The number of rows deleted from the database as a result of internal activity.
int_rows_updated	The number of rows updated from the database as a result of internal activity.
int_rows_inserted	The number of rows inserted into the database as a result of internal activity caused by triggers.
static_sql_stmts	The number of static SQL statements that were attempted.
dynamic_sql_stmts	The number of dynamic SQL statements that were attempted.
failed_sql_stmts	The number of SQL statements that were attempted, but failed.
commit_sql_stmts	The total number of SQL COMMIT statements that have been attempted.
rollback_sql_stmts	The total number of SQL ROLLBACK statements that have been attempted.
select_sql_stmts	The number of SQL SELECT statements that were executed.
uid_sql_stmts	The number of SQL UPDATE, INSERT, and DELETE statements that were executed.
ddl_sql_stmts	The number of SQL Data Definition Language (DDL) statements that were executed.
int_auto_rebinds	The number of automatic rebinds (or recompiles) that have been attempted.

Measurement	Description
int_commits	The total number of commits initiated internally by the database manager.
int_rollbacks	The total number of rollbacks initiated internally by the database manager.
int_deadlock_rollbacks	The total number of forced rollbacks initiated by the database manager due to a deadlock. A rollback is performed on the current unit of work in an application selected by the database manager to resolve the deadlock.
binds_precompiles	The number of binds and pre-compiles attempted.

Application

The following table lists the Application counters:

Measurement	Description
agents_stolen	The number of times that agents are stolen from an application. Agents are stolen when an idle agent associated with an application is reassigned to work on a different application.
num_assoc_agents	At the application level, this is the number of sub-agents associated with an application. At the database level, it is the number of sub-agents for all applications.
total_sorts	The total number of sorts that have been executed.
total_sort_time	The total elapsed time (in milliseconds) for all sorts that have been executed.
sort_overflows	The total number of sorts that ran out of sort heap and may have required disk space for temporary storage.
total_hash_joins	The total number of hash joins executed.

Measurement	Description
total_hash_loops	The total number of times that a single partition of a hash join was larger than the available sort heap space.
hash_join_overflows	The number of times that hash join data exceeded the available sort heap space
hash_join_small_overflows	The number of times that hash join data exceeded the available sort heap space by less than 10%.
pool_data_l_reads	The number of logical read requests for data pages that have gone through the buffer pool.
pool_data_p_reads	The number of read requests that required I/O to get data pages into the buffer pool.
pool_data_writes	The number of times a buffer pool data page was physically written to disk.
pool_index_l_reads	The number of logical read requests for index pages that have gone through the buffer pool.
pool_index_p_reads	The number of physical read requests to get index pages into the buffer pool.
pool_index_writes	The number of times a buffer pool index page was physically written to disk.
pool_read_time	Provides the total amount of elapsed time spent processing read requests that caused data or index pages to be physically read from disk to buffer pool.
prefetch_wait_time	The time an application spent waiting for an I/O server (pre-fetcher) to finish loading pages into the buffer pool.
pool_data_to_estore	The number of buffer pool data pages copied to extended storage.
pool_index_to_estore	The number of buffer pool index pages copied to extended storage.
pool_data_from_estore	The number of buffer pool data pages copied from extended storage.

Measurement	Description
pool_index_from_estore	The number of buffer pool index pages copied from extended storage.
direct_reads	The number of read operations that do not use the buffer pool.
direct_writes	The number of write operations that do not use the buffer pool.
direct_read_reqs	The number of requests to perform a direct read of one or more sectors of data.
direct_write_reqs	The number of requests to perform a direct write of one or more sectors of data.
direct_read_time	The elapsed time (in milliseconds) required to perform the direct reads.
direct_write_time	The elapsed time (in milliseconds) required to perform the direct writes.
cat_cache_lookups	The number of times that the catalog cache was referenced to obtain table descriptor information.
cat_cache_inserts	The number of times that the system tried to insert table descriptor information into the catalog cache.
cat_cache_overflows	The number of times that an insert into the catalog cache failed due to the catalog cache being full.
cat_cache_heap_full	The number of times that an insert into the catalog cache failed due to a heap-full condition in the database heap.
pkg_cache_lookups	The number of times that an application looked for a section or package in the package cache. At a database level, it indicates the overall number of references since the database was started, or monitor data was reset.

Measurement	Description
pkg_cache_inserts	The total number of times that a requested section was not available for use and had to be loaded into the package cache. This count includes any implicit prepares performed by the system.
appl_section_lookups	Lookups of SQL sections by an application from its SQL work area.
appl_section_inserts	Inserts of SQL sections by an application from its SQL work area.
uow_log_space_used	The amount of log space (in bytes) used in the current unit of work of the monitored application.
locks_held	The number of locks currently held.
deadlocks	The total number of deadlocks that have occurred.
lock_escals	The number of times that locks have been escalated from several row locks to a table lock.
x_lock_escals	The number of times that locks have been escalated from several row locks to one exclusive table lock, or the number of times an exclusive lock on a row caused the table lock to become an exclusive lock.
lock_timeouts	The number of times that a request to lock an object timed-out instead of being granted.
lock_waits	The total number of times that applications or connections waited for locks.
lock_wait_time	The total elapsed time waited for a lock.
locks_waiting	Indicates the number of agents waiting on a lock.
uow_lock_wait_time	The total amount of elapsed time this unit of work has spent waiting for locks.
rows_deleted	The number of row deletions attempted.

Measurement	Description
rows_inserted	The number of row insertions attempted.
rows_updated	The number of row updates attempted.
rows_selected	The number of rows that have been selected and returned to the application.
rows_written	The number of rows changed (inserted, deleted or updated) in the table.
rows_read	The number of rows read from the table.
int_rows_deleted	The number of rows deleted from the database as a result of internal activity.
int_rows_updated	The number of rows updated from the database as a result of internal activity.
int_rows_inserted	The number of rows inserted into the database as a result of internal activity caused by triggers.
open_rem_curs	The number of remote cursors currently open for this application, including those cursors counted by 'open_rem_curs_blk'.
open_rem_curs_blk	The number of remote blocking cursors currently open for this application.
rej_curs_blk	The number of times that a request for an I/O block at server was rejected and the request was converted to non-blocked I/O.
acc_curs_blk	The number of times that a request for an I/O block was accepted.
open_loc_curs	The number of local cursors currently open for this application, including those cursors counted by 'open_loc_curs_blk'.
open_loc_curs_blk	The number of local blocking cursors currently open for this application.
static_sql_stmts	The number of static SQL statements that were attempted.

Measurement	Description
dynamic_sql_stmts	The number of dynamic SQL statements that were attempted.
failed_sql_stmts	The number of SQL statements that were attempted, but failed.
commit_sql_stmts	The total number of SQL COMMIT statements that have been attempted.
rollback_sql_stmts	The total number of SQL ROLLBACK statements that have been attempted.
select_sql_stmts	The number of SQL SELECT statements that were executed.
uid_sql_stmts	The number of SQL UPDATE, INSERT, and DELETE statements that were executed.
ddl_sql_stmts	The number of SQL Data Definition Language (DDL) statements that were executed.
int_auto_rebinds	The number of automatic rebinds (or recompiles) that have been attempted.
int_commits	The total number of commits initiated internally by the database manager.
int_rollbacks	The total number of rollbacks initiated internally by the database manager.
int_deadlock_rollbacks	The total number of forced rollbacks initiated by the database manager due to a deadlock. A rollback is performed on the current unit of work in an application selected by the database manager to resolve the deadlock.
binds_precompiles	The number of binds and pre-compiles attempted.

25

Oracle Monitoring

The Oracle monitor displays information from Oracle V$ tables: Session statistics, V$SESSTAT, system statistics, V$SYSSTAT, and other table counters defined by the user in the custom query.

The SiteScope Oracle JDBC Monitor monitors the server performance statistics from Oracle Database servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. You can create a separate Oracle JDBC Monitor instance for each Oracle database server in your environment.

To obtain data for this graph, you must first set up the monitoring environment. You then configure the Oracle online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

This chapter includes:

Note: The port you use to monitor an Oracle server through a firewall depends on the configuration of the Oracle server. Configuration information for the connection between the client and server is located in the Oracle client **tnsnames.ora** file.

Setting Up the Monitoring Environment

- If you are using the SiteScope monitor engine, ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.
- The Oracle server measures information from the V$SESSTAT and V$SYSSTAT Oracle V$ tables, and other table counters defined by the user in the custom query. In order to monitor the Oracle server, you must set up the monitoring environment as described below before you can configure the monitor.

To set up the native LoadRunner Oracle monitor environment:

1. Ensure that the Oracle client libraries are installed on the Controller machine.
2. Verify that **%OracleHome%\bin** is included in the path environment variable. If it is not, add it.
3. Configure the **tnsnames.ora** file on the Controller machine so that the Oracle client can communicate with the Oracle server(s) you plan to monitor.

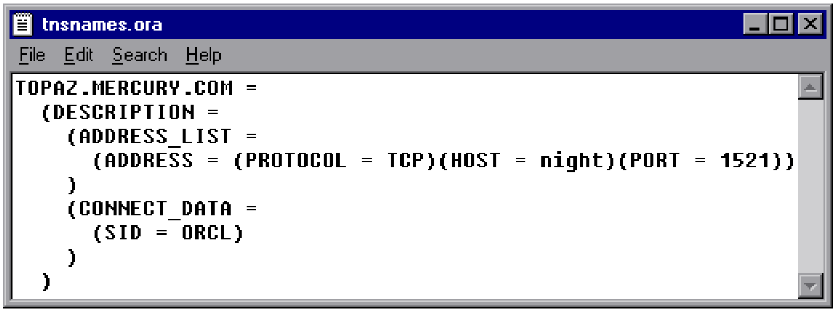
   You can configure connection parameters either manually, by editing the **tnsnames.ora** file in a text editor, or using the Oracle service configuration tool (for example, select **Start** > **Programs** > **Oracle for Windows NT** > **Oracle Net8 Easy Config**).

   You specify:

   - a new service name (TNS name) for the Oracle instance
   - TCP protocol

- the host name (name of monitored server machine)
- the port number (usually 1521)
- the database SID (the default SID is ORCL)

For example:



```
TOPAZ.MERCURY.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = night)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ORCL)
    )
  )
```

Note: Only the 32-bit Oracle client should be installed on the Controller machine running the Oracle monitor. If you have a 16-bit and a 32-bit Oracle client installation on the Controller machine, the 16-bit installation should be uninstalled.

---

4. Obtain a username and password for the service from your database administrator, and ensure that the Controller has database administrator privileges for the Oracle V$tables (V$SESSTAT, V$SYSSTAT, V$STATNAME, V$INSTANCE, V$SESSION).
5. Verify connection with the Oracle server by performing **tns ping** from the Controller machine.

Note: here may be a problem connecting if the Oracle server is behind a DMZ/firewall that limits its communication to application servers accessing it.

---

6. Ensure that the registries are updated for the version of Oracle that you are using and that they have the following key:
   HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
7. Verify that the Oracle server you want to monitor is up and running.

Note: It is possible to monitor several Oracle database servers concurrently.

---

8. Run SQL*Plus from the Controller and attempt to log in to the Oracle server(s) with the desired username/password/server combination.
9. Type SELECT * FROM V$SYSSTAT to verify that you can view the V$SYSSTAT table on the Oracle server. Use similar queries to verify that you can view the V$SESSTAT, V$SESSION, V$INSTANCE, V$STATNAME, and V$PROCESS tables on the server. Make sure that the Oracle **bin** directory is in the search path.
10. To change the length of each monitoring sample (in seconds), you need to edit the **dat\monitors\vmon.cfg** file in the LoadRunner root folder. The default rate is 10 seconds.

Note: The minimum sampling rate for the Oracle Monitor is 10 seconds. If you set the sampling rate at less than 10 seconds, the Oracle Monitor will continue to monitor at 10 second intervals.

If a problem occurs in setting up the Oracle environment, view the error message issued by the Oracle server.

To set up the SiteScope Oracle JDBC monitor environment:

1 You must have a copy of the applicable Oracle JDBC database driver file (for example, **classes12.zip**) on the SiteScope server.

Copy the downloaded driver file into the <**SiteScope install path**>**SiteScope****java****lib****ext** subdirectory. DO NOT unzip the file.

Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

Note: More than one driver file is available for download. Some drivers support more than one version of Oracle database (for example, the **classes12.zip** Oracle JDBC thin driver) while others only support a particular version. If you are monitoring a recent version of Oracle database, you should download the latest version of the database driver.

---

2 You must supply the correct Database Connection URL, a database username and password when setting up the monitor. The syntax of the Database Connection URL usually has the form of:

```
jdbc:oracle:thin:@<tcp address>:<tcp port>:<database sid>.
```

For example to connect to the ORCL database on a machine using port 1521 you would use:

```
jdbc:oracle:thin:@206.168.191.19:1521:ORCL
```

Note: The colon and @ symbols must be included as shown.

---

3 You must specify the Oracle Database Driver that was installed on the SiteScope server when setting up the monitor. The Database Driver for the Oracle thin JDBC driver is:

```
oracle.jdbc.driver.OracleDriver
```

4 You should only have one Oracle client installed on the SiteScope machine. If there is more that one client installed, SiteScope may report an error and be unable to connect to the database.

5 You must have an Oracle user login that SiteScope will use to access the Oracle server. In order to retrieve the Oracle database counters, the user that SiteScope will use for the Oracle JDBC Monitor should be able to execute all the SQL statements as found in the file **SiteScope\templates.applications\commands.oraclejdbc**.

Adding a Machine to Monitor

In order to monitor the Oracle database resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller

1 Click the Oracle graph in the graph tree, and drag it into the right pane of the Run view.

2 Right-click the graph and select **Add Measurements**, or click anywhere on graph and choose **Monitors** > **Add Measurements**. The Oracle dialog box opens.

3 By default, LoadRunner monitors Oracle database resources using the native LoadRunner monitor engine.

If you want to monitor the Oracle database using a SiteScope monitor, click **Advanced**.

In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK** to close the Monitor Engine dialog box.

4 In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

- In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs.
- In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

  Note: If you are adding a native LoadRunner monitor, the **SiteScope Server Information** section does not appear.

Click **OK** to close the Add Machine dialog box.

5 In the **Resource Measurements on:** <*machine*> section of the Oracle dialog box, click **Add**.

6 Continue with Configuring the Oracle Monitor below.

Configuring the Oracle Monitor

The configuration for this monitor differs slightly depending on whether you are adding a SiteScope or native LoadRunner monitor.

This section describes:

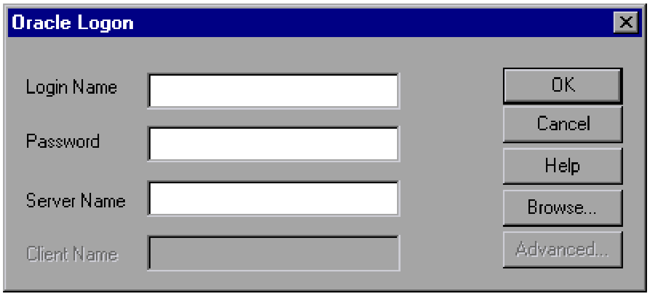
- Configuring the Native LoadRunner Oracle Database Monitor
- Configuring the SiteScope Oracle JDBC Monitor

Configuring the Native LoadRunner Oracle Database Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which objects to monitor on the machine.

To configure the Oracle Database monitor:

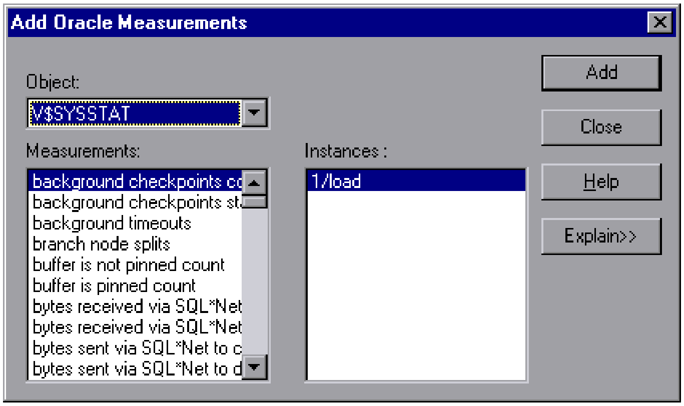
1 When you click Add to add a measurement, the Oracle Logon dialog box opens.



Enter the following information, and then click **OK.**

- **Login Name.** Enter your login name.
- **Password.** Enter your password.
- **Server Name.** Enter the name of the server.

2 The Add Oracle Measurements dialog box opens, displaying the available measurements.



3 For each measurement, select an object, measurement, and instance, and then click **Add**, as described in "Understanding the Add Oracle Measurements Dialog Box" below.

For a description of the available measurements, see "Oracle Performance Counters" on page 247.

4 Click **Close**. The measurements that you selected appear in the **Resource Measurements on**: *<machine>* section of the Oracle dialog box.

5 Click **OK** in the Oracle dialog box to activate the monitor.

Note: By default, the database returns the absolute value of a counter. However, by changing the IsRate setting in the **dat\monitors\vmon.cfg** file to 1, you can instruct the database to report a counter's rate value—the change in the counter per unit time.

Understanding the Add Oracle Measurements Dialog Box

The Add Oracle Measurements dialog box lets you select the resources to monitor from the V$SESSTAT and V$SYSSTAT Oracle V$ tables.

➤ **Object.** Select the object being monitored on the specified machine.

- **Measurements.** Select a resource measurement to monitor. Select multiple measurements using the CTRL key. For an explanation of each measurement, click **Explain**.
- **Instances.** If multiple instances of the selected measurement are running, select one or more instances to monitor for the selected measurement.
- **Explain.** Displays a description of the selected measurement.

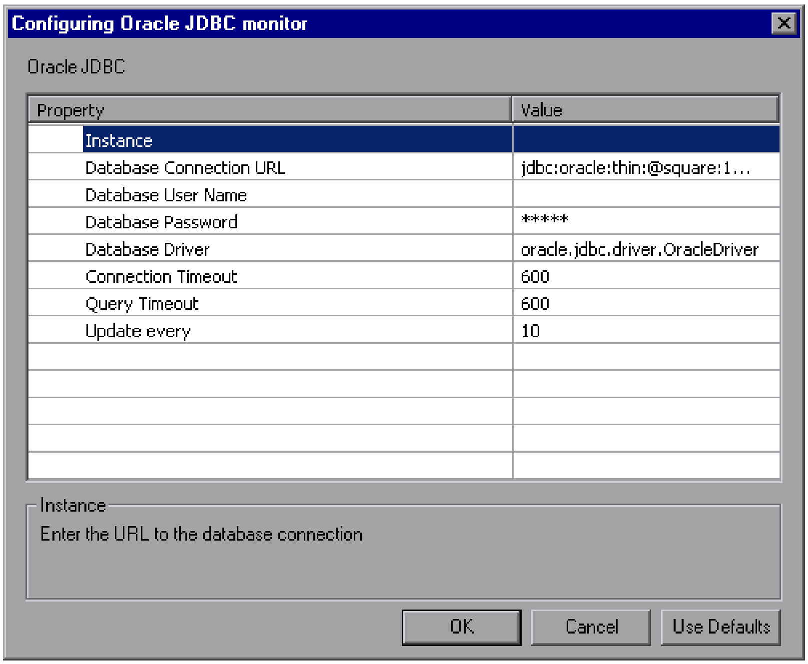
Configuring the SiteScope Oracle JDBC Monitor

After you have added the machine that you are monitoring, you choose the measurements to monitor on the machine.

To configure the Oracle JDBC monitor:

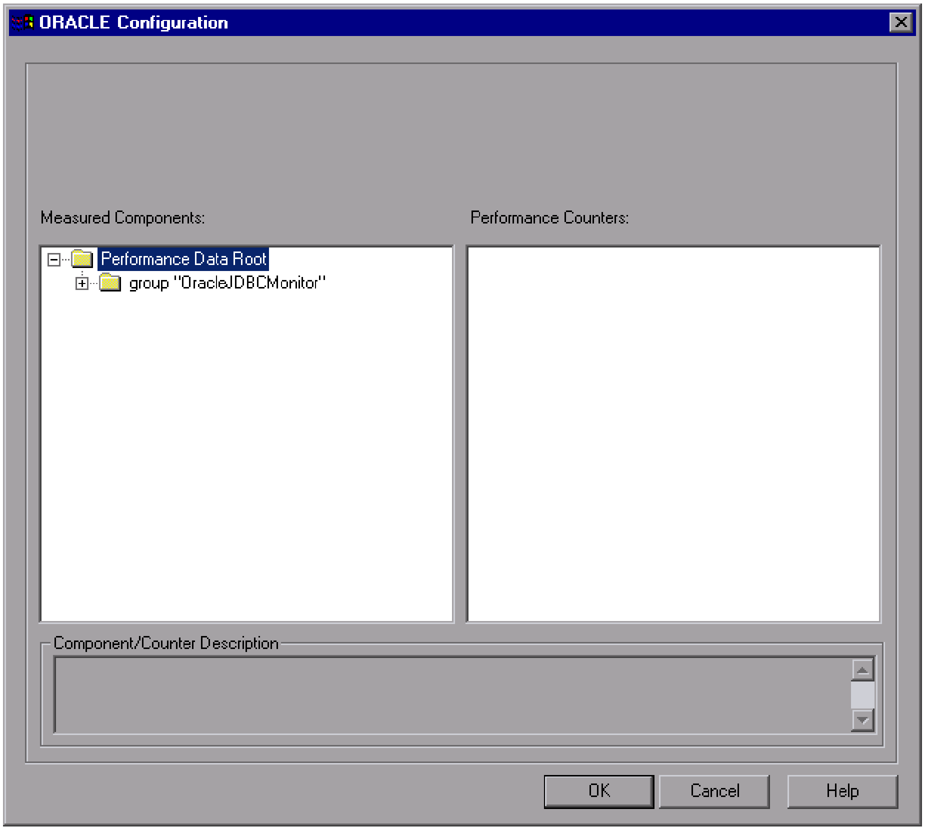
1 The first time you add a measurement to the monitor, you need to configure the monitor properties. When you click **Add** to add a measurement, the Configuring Oracle JDBC Monitor dialog box opens.

Enter values for the monitor properties as described in "Understanding the Configuring Oracle JDBC Monitor Dialog Box" on page 246, and click **OK**.



2 The Oracle Configuration dialog box opens.

Browse the **Measured Components** tree and select the performance counters on the right, as described in "Understanding the Oracle Configuration Dialog Box" on page 247. Click a component or counter to see its description in the **Component/Counter Description** section.



3 Click **OK** to close the Oracle Configuration dialog box. The components that you selected appear in the **Resource Measurements on**: *<machine>* section of the Oracle dialog box.

4 Click **OK** in the Oracle dialog box to activate the monitor.

Understanding the Configuring Oracle JDBC Monitor Dialog Box

You use the Configuring Oracle JDBC Monitor dialog box to configure the Oracle JDBC monitor.

- **Instance.** Enter the database SID. For example, ORCL.
- **Database Connection URL.** Enter the connection URL to the database you want to monitor. For example, jdbc:oracle:thin:@206.168.191.19:1521:ORCL
- **Database User Name.** Enter the user name that SiteScope should use to connect to the database.
- **Database Password.** Enter the password for the user name that SiteScope should use to connect to the database.
- **Database Driver.** Enter the driver used to connect to the database. For example, oracle.jdbc.driver.OracleDriver.
- **Connection Timeout.** Enter an optional the time out value, in seconds, that SiteScope should to wait for a database connection to respond.
- **Query Timeout.** Enter an optional the time out value, in seconds, that SiteScope should to wait for a response from the database query. If the database does not respond within the period specified, SiteScope will report an error.
- **Update every.** Select how often the monitor should read the server statistics. The default interval is to run or update the monitor once every 10 seconds.

Notes:

- The sum of the **Connection Timeout** value and **Query Timeout** value should always be less than the **Update every** value for the monitor.
- Some commonly used databases and database drivers do not support the Query Timeout feature. In these cases the Query Timeout value should be set to zero.

Understanding the Oracle Configuration Dialog Box

The Oracle Configuration dialog box enables you to select the performance counters to monitor.

➤ **Host.** The name of the host machine.

➤ **Measured Components.** Displays a tree containing all the available measured components.

➤ **Performance Counters.** Displays the performance counters for a selected measured component.

➤ **Component/Counter Description.** Displays a description of the selected measured component or performance counter.

Oracle Performance Counters

The following measurements are most commonly used when monitoring the Oracle server (from the V$SYSSTAT table):

Measurement	Description
CPU used by this session	The amount of CPU time (in 10s of milliseconds) used by a session between the time a user call started and ended. Some user calls can be completed within 10 milliseconds and, as a result, the start and end-user call time can be the same. In this case, 0 milliseconds are added to the statistic. A similar problem can exist in the operating system reporting, especially on systems that suffer from many context switches.
Bytes received via SQL*Net from client	The total number of bytes received from the client over Net8.
Logons current	The total number of current logons
Opens of replaced files	The total number of files that needed to be reopened because they were no longer in the process file cache.

Measurement	Description
User calls	Oracle allocates resources (Call State Objects) to keep track of relevant user call data structures every time you log in, parse, or execute. When determining activity, the ratio of user calls to RPI calls gives you an indication of how much internal work is generated as a result of the type of requests the user is sending to Oracle.
SQL*Net roundtrips to/from client	The total number of Net8 messages sent to, and received from, the client.
Bytes sent via SQL*Net to client	The total number of bytes sent to the client from the foreground process(es).
Opened cursors current	The total number of current open cursors.
DB block changes	Closely related to consistent changes, this statistic counts the total number of changes that were made to all blocks in the SGA that were part of an update or delete operation. These are changes that generate redo log entries and hence will cause permanent changes to the database if the transaction is committed. This statistic is a rough indication of total database work and indicates (possibly on a per-transaction level) the rate at which buffers are being dirtied.
Total file opens	The total number of file opens being performed by the instance. Each process needs a number of files (control file, log file, database file) to work against the database.

Custom Queries

Using the custom query feature, you can define your own query to the Oracle database and view the result of this query—a single numerical value—in the Oracle online monitor graph. By defining your own query, you can monitor not only the V$SYSSTAT and V$SESSTAT table counters that are currently provided by the Oracle monitor, but other tables that contain useful performance information as well.

To create a custom query:

1. In the third line of the **vmon.cfg** file, CustomCounters=, indicate the number of custom counters you want to create.
2. Create a new section in the **vmon.cfg** file for the new counter. Each section has the following format:

   ```
   [Custom2]
   Name=Number of sessions
   Description=This counter returns the number of sessions active.
   Query=SELECT COUNT(*) FROM V$SESSION
   IsRate=1
   ```

3. In the [Custom#] line, assign the next number in the sequence of counters to the new custom counter. The custom counters must be in consecutive order, beginning with the number 0.
4. In the Name line, enter the name of the new counter.
5. In the Description line, enter the description of the counter that you want the help message to contain.
6. In the Query line, enter the text of the SQL query (on one line of the **vmon.cfg** file) that returns exactly one row from the database. This row must contain one column, a numerical value. Custom queries should not exceed 512 characters.
7. In the IsRate line, enter 0 if you want the database to report the counter as an absolute number. If you want the database to report the change in the counter per unit time, enter 1. Custom queries cannot return negative values.

26

SQL Server Monitoring

The SQL Server monitor shows the standard Windows resources on the SQL server machine.

Note: To monitor an SQL server through a firewall, use TCP, port 139.

This chapter includes:

Setting up the Monitoring Environment

- ➤ If you are using the SiteScope monitor engine, ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.
- ➤ To obtain data for this graph, you enable the SQL Server online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

Adding a Machine to Monitor

In order to monitor the SQL Server resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller

1 Click **SQL Server** in the graph tree, and drag it into the right pane of the Run view.

2 Right-click the graph and select **Add Measurements**, or click anywhere on graph and choose **Monitors** > **Add Measurements**. The SQL Server dialog box opens.

3 By default, LoadRunner monitors SQL Server resources using the native LoadRunner monitor engine.

If you want to monitor the SQL Server using a SiteScope monitor, click **Advanced**.

In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK** to close the Monitor Engine dialog box.

4 In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

➤ In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs.

➤ In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

Note: If you are adding a native LoadRunner monitor, the **SiteScope Server Information** section does not appear.

Click **OK** to close the Add Machine dialog box.

5 Click **Add** in the **Resource Measurements on:** *<machine>* section of the SQL Server dialog box

6 Continue with Configuring the SQL Server Monitor below.

Configuring the SQL Server Monitor

The configuration for this monitor differs slightly depending on whether you are adding a SiteScope or native LoadRunner monitor.

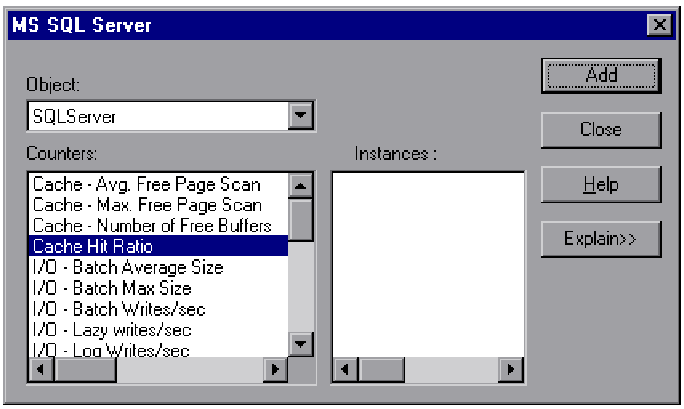
Configuring the Native LoadRunner SQL Server Monitor

1 When you add a machine in the SQL Server dialog box, the default measurements are displayed in the **Resource Measurements on:** *<machine>* section.

Note: To change the default counters for the SQL Server monitor, see “Changing a Monitor’s Default Counters” on page 395.

- To delete a measurement from the default list, select the measurement and click **Delete**.
- To select additional measurements, click **Add**.

2 The MS SQL Server dialog box opens displaying the SQL Server resources.



For each measurement select an object, counter, and instance, as described in “Understanding the Add MS SQL Server Measurements Dialog Box” on page 254, and then click **Add**.

For a description of the available measurements, see “SQL Server Performance Counters” on page 256.

3 When you have finished selecting the measurements to monitor, click **Close**. The counters that you selected appear in the **Resource Measurements on**: *<machine>* section of the SQL Server dialog box.

4 Click **OK** in the SQL Server dialog box to activate the monitor.

Note: Certain measurements or counters are especially useful for determining server performance and isolating the cause of a bottleneck during an initial stress test on the SQL Server. For more information about these counters, see “Useful Counters for Stress Testing” on page 396.

Understanding the Add MS SQL Server Measurements Dialog Box

The Add MS SQL Server Measurements dialog box lets you select additional resources to monitor on the SQL Server.

- **Object.** Select the object being monitored on the specified machine.
- **Counters/Measurements.** Select a resource counter/measurement to monitor. Select multiple counters using the CTRL key. For an explanation of each counter/measurement, click **Explain**.
- **Instances.** If multiple instances of the selected counter/measurement are running, select one or more instances to monitor for the selected counter/measurement.
- **Explain/Collapse.** Displays/Collapses the Measurement Description box that describes the selected counter/measurement.

Configuring the SiteScope SQL Server Monitor

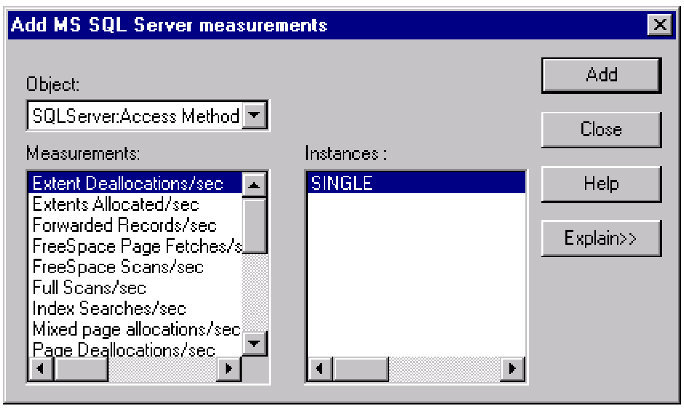
1 The first time you add measurements you need to configure the remote machine properties. When you click **Add** in the **Resource Measurements on:** <*machine*> section of the SQL Server dialog box, a dialog box opens to configure the remote machine as follows:

- ➤ If you are monitoring a machine on a UNIX platform, the Configuring UNIX Remote Machine dialog box opens.
- ➤ If you are monitoring a machine on a Windows platform, the Configuring NT Remote Machine dialog box opens.

Enter the remote machine's configuration information, as described in "Configuring the Remote Machine for SiteScope Monitors" on page 25, and click **OK**.

2 The Configuring SQL Server Monitor dialog box opens. Verify the **Server** and **Update every** properties, and click **OK**.

3 The Add MS SQL Server Measurements dialog box opens displaying the available measurements and server properties.



For each measurement select an object, measurement, and instance, as described in "Understanding the Add MS SQL Server Measurements Dialog Box" on page 254, and then click **Add**.

For a description of the available measurements, see "SQL Server Performance Counters" on page 256.

4 When you have finished selecting the measurements to monitor, click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the SQL Server dialog box.

5 Click **OK** in the SQL Server dialog box to activate the monitor.

SQL Server Performance Counters

The following table describes the default counters that can be monitored on version 6.5 of the SQL Server:

Measurement	Description
% Total Processor Time	The average percentage of time that all the processors on the system are busy executing non-idle threads. On a multi-processor system, if all processors are always busy, this is 100%, if all processors are 50% busy this is 50% and if 1/4 of the processors are 100% busy this is 25%. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process which consumes those unproductive processor cycles not used by any other threads.
% Processor Time	The percentage of time that the processor is executing a non-idle thread. This counter was designed as a primary indicator of processor activity. It is calculated by measuring the time that the processor spends executing the thread of the idle process in each sample interval, and subtracting that value from 100%. (Each processor has an idle thread which consumes cycles when no other threads are ready to run). It can be viewed as the percentage of the sample interval spent doing useful work. This counter displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time the service was inactive, and then subtracting that value from 100%.
Cache Hit Ratio	The percentage of time that a requested data page was found in the data cache (instead of being read from disk).

Measurement	Description
I/O - Batch Writes/sec	The number of 2K pages written to disk per second, using Batch I/O. The checkpoint thread is the primary user of Batch I/O.
I/O - Lazy Writes/sec	The number of 2K pages flushed to disk per second by the Lazy Writer.
I/O - Outstanding Reads	The number of physical reads pending.
I/O - Outstanding Writes	The number of physical writes pending.
I/O - Page Reads/sec	The number of physical page reads per second.
I/O - Transactions/sec	The number of Transact-SQL command batches executed per second.
User Connections	The number of open user connections.

Part X

Streaming Media Monitoring

27

Introduction to Streaming Media Monitoring

To isolate server and client performance bottlenecks during a scenario run, you monitor the Windows Media Server and RealPlayer audio/video servers, as well as the RealPlayer and Media Player clients.

Note: For instructions on recording a script containing streaming media functions, see the HP Virtual User Generator.

The streaming media monitors provide you with performance information for the Windows Media Server and RealPlayer audio/video servers, as well as the RealPlayer and Media Player clients. To obtain data for the Windows Media Server and RealPlayer Server, you need to activate the streaming media monitor before executing the scenario, and indicate which statistics and measurements you want to monitor. The RealPlayer Client and Media Player Client do not require pre-session or scenario activation or configuration.

28

RealPlayer Client Monitoring

The Real Client monitor shows statistics on the RealPlayer client machine as a function of the elapsed scenario time. The x-axis represents the time that has elapsed since the start of the scenario run. The y-axis represents the resource usage.

This chapter includes:

Configuring the Real Client Monitor

You can view the RealPlayer Client online monitor graph by dragging it from the graph tree into the right pane of the Run view. The graph appears in the graph view area.

RealPlayer Client Performance Counters

The following table describes the RealPlayer Client measurements that are monitored:

Measurement	Description
Current Bandwidth (Kbits/sec)	The number of kilobytes in the last second
Buffering Event Time (sec)	The average time spent on buffering
Network Performance	The ratio (percentage) between the current bandwidth and the actual bandwidth of the clip
Percentage of Recovered Packets	The percentage of error packets that were recovered
Percentage of Lost Packets	The percentage of packets that were lost
Percentage of Late Packets	The percentage of late packets
Time to First Frame Appearance (sec)	The time for first frame appearance (measured from the start of the replay)
Number of Buffering Events	The average number of all buffering events
Number of Buffering Seek Events	The average number of buffering events resulting from a seek operation
Buffering Seek Time	The average time spent on buffering events resulting from a seek operation
Number of Buffering Congestion Events	The average number of buffering events resulting from network congestion
Buffering Congestion Time	The average time spent on buffering events resulting from network congestion

Measurement	Description
Number of Buffering Live Pause Events	The average number of buffering events resulting from live pause
Buffering Live Pause Time	The average time spent on buffering events resulting from live pause

29

Media Player Client Monitoring

The Media Player Client monitor graph shows statistics on the Windows Media Player client machine as a function of the elapsed scenario time. The x-axis represents the time that has elapsed since the start of the scenario run. The y-axis represents the resource usage.

This chapter includes:

Configuring the Windows Media Player Client Monitor

The Windows Media Player Client online monitor graph is only available during scenarios that run Windows Media Player scripts.

You can view this graph by dragging it from the graph tree into the right pane of the Run view. The graph appears in the graph view area.

Media Player Client Performance Counters

The following table describes the Media Player Client measurements that are monitored:

Measurement	Description
Average Buffering Events	The number of times Media Player Client had to buffer incoming media data due to insufficient media content.
Average Buffering Time (sec)	The time spent by Media Player Client waiting for sufficient amount of media data in order to continue playing media clip.
Current bandwidth (Kbits/sec)	The number of kbits per second received.
Number of Packets	The number of packets sent by server for a particular media clip.
Stream Interruptions	The number of interruptions encountered by media player client while playing a media clip. This measurement includes the number of times Media Player Client had to buffer incoming media data, and any errors that occurred during playback.
Stream Quality (Packet-level)	The percentage ratio of packets received to total packets.
Stream Quality (Sampling-level)	The percentage of stream samples received on time (no delays in reception).
Total number of recovered packets	The number of lost packets that were recovered. This value is only relevant during network playback.
Total number of lost packets	The number of lost packets that were not recovered. This value is only relevant during network playback.

Part XI

ERP/CRM Server Resource Monitoring

30

Introduction to ERP/CRM Server Resource Monitoring

You use LoadRunner's ERP/CRM server resource monitors to monitor ERP/CRM servers during a scenario run and isolate server performance bottlenecks.

This chapter includes:

About ERP/CRM Server Resource Monitoring

The ERP/CRM server resource monitors provide you with performance information for ERP/CRM servers. To display this data, you must activate the monitors before executing the scenario and select the statistics and measurements you want to monitor.

Choosing Between Different SAP Monitors

You can monitor the resource usage of SAP solutions R/3, BW, CRM, APO, SAP Enterprise Portal, and SAPGUI for HTML during a scenario run using the SAP server monitors. Use the support matrix below to help you select the appropriate SAP monitor.

Support Matrix

SAP Application	Server Release	LoadRunner Monitor	Required SAPGUI
➤ R/3 3.1-4.6D ➤ BW 2.x	SAP R/3 Kernel 3.1-4.6D (based on the SAP Application Server)	➤ SAP CCMS Monitor	SAPGUI 3.1-6.20
➤ R/3 4.7 Enterprise ➤ BW 3.1 ➤ CRM 4.0 ➤ APO 3.x	SAP R/3 Kernel WAS 6.20 (based on the SAP Web Application Server)	➤ SAPGUI Monitor ➤ SAP CCMS Monitor	SAPGUI 6.20

SAP Application	Server Release	LoadRunner Monitor	Required SAPGUI
SAP Enterprise Portal	No SAP System integration	➤ SAP Portal Monitor	
	SAP 3.1-4.6 kernel based SAP System integration	➤ SAP CCMS Monitor ➤ SAP Portal Monitor	LoadRunner Controller machine: SAPGUI 3.1-6.20 (see note below)
	SAP 6.20 kernel based SAP System integration	➤ SAPGUI Monitor ➤ SAP CCMS Monitor ➤ SAP Portal Monitor	LoadRunner Controller machine: SAPGUI 6.20 (see note below)
SAPGUI for HTML	SAP 3.1-4.6 kernel based SAP System integration	➤ SAP CCMS Monitor	LoadRunner Controller machine: SAPGUI 3.1-6.20 (see note below)
	SAP 6.20 kernel based SAP System integration	➤ SAPGUI Monitor ➤ SAP CCMS Monitor	LoadRunner Controller machine: SAPGUI 6.20 (see note below)

Note: A connection from the Controller to the SAP System using SAPGUI is only required for monitoring purposes. SAPGUI is not required on the load generator machines.

31

SAP Portal Server Resource Monitoring

The SAP Portal monitor displays statistics about the resource usage of an SAP Enterprise Portal environment during the scenario run.

To obtain data on the SAP R/3 system server, you need to configure the SAP online monitor (from the Controller) before executing the scenario, and indicate which statistics and measurements you want to monitor. You select these counters using the SAP Portal dialog box.

This chapter includes:

Setting up the Monitoring Environment

Before monitoring an SAP Portal server:

➤ Ensure that SiteScope has been installed on a server. You can install it on the same machine as the Controller, or on a dedicated server.

Adding a Machine to Monitor

In order to monitor the SAP Portal resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the SAP Portal graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The SAP Portal dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

   ➤ In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor, and select the platform on which the machine runs.

   ➤ In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

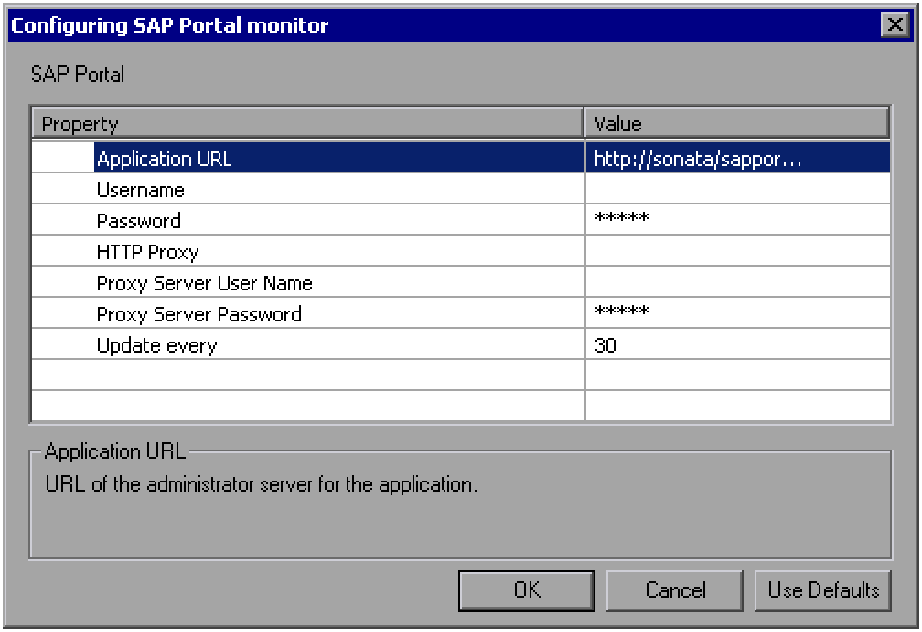
   Click **OK**. The SAP Portal dialog box is redisplayed.
3. In the **Resource Measurements** section, click **Add**.
4. Continue with Configuring the SAP Portal Monitor below.

Configuring the SAP Portal Monitor

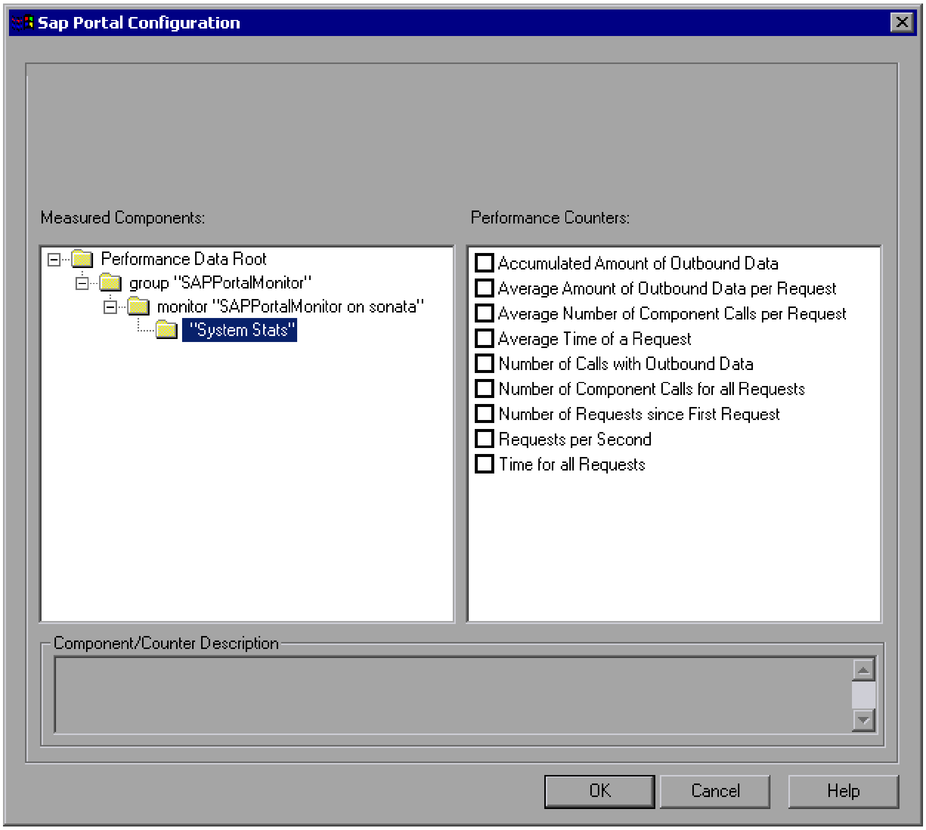
After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the SAP Portal monitor:

1 When you click **Add** to add a measurement, the Configuring SAP Portal Monitor dialog box opens. Enter the SAP Portal monitor information, as described in "Understanding the Configuring SAP Portal Monitor Dialog Box" on page 279.



2 Click **OK**. The SAP Portal Configuration dialog box opens, displaying the available measurements.



3 Browse the Measured Components tree, and select performance counters, as described in "Understanding the SAP Portal Configuration Dialog Box" on page 279.

For a description of the available measurements, see "SAP Portal Performance Counters" on page 280.

4 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the SAP Portal dialog box.

5 Click **OK** in the SAP Portal dialog box, to activate the monitor.

Note: The minimum recommended SiteScope monitor refresh rate is 30 seconds. If you choose a lower refresh rate, the Controller may not get all the data in time.

Understanding the Configuring SAP Portal Monitor Dialog Box

The Configuring SAP Portal Monitor Dialog Box enables you to configure the SAP Portal monitor.

- **Application URL.** Enter the URL of the administrator server for the application.
- **Username.** Enter the user name for the server administrator page.
- **Password.** Enter the password for the server administrator page.
- **HTTP Proxy.** Enter a proxy server to use, including the port (optional).
- **Proxy Server User Name.** If the proxy server requires authorization, enter the user name.
- **Proxy Server Password.** If the proxy server requires authorization, enter the password.
- **Update every.** Enter the amount of time lapse between the SiteScope check of the monitor.

Understanding the SAP Portal Configuration Dialog Box

The SAP Portal dialog box enables you to select the SAP Portal resources to monitor.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.

- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

SAP Portal Performance Counters

The following table shows the default counters that can be measured:

Measurement	Description
Accumulated Amount of Outbound Data (bytes)	The accumulated amount of outbound data, measured in bytes.
Average Amount of Outbound Data per Request (bytes)	The average amount of outbound data per request, measured in bytes.
Average Number of Component Calls per Request (bytes)	The average number of component calls per request, measured in bytes.
Average Time of a Request (ms)	The average amount of time, in milliseconds, taken to process a request.
Number of Calls with Outbound Data	The total number of calls with outbound data.
Number of Component Calls for all Requests	The total number of component calls for all requests.
Number of Requests since First Request	The total number of requests since the first request was made.
Requests per Second	The number of requests made per second.
Time for all Requests (ms)	The total time, in milliseconds, taken for processing all requests.

32

SAP CCMS Resource Monitoring

The SAP CCMS (Computer Center Management System) monitor displays statistics about the resource usage of all servers, components, and resources in any SAP R/3 landscape during the scenario run. You can also use the SAP CCMS monitor for SAP Portal and SAP GUI environments, but the amount of measurements provided by the SAP CCMS monitor is much greater.

To obtain data on the SAP R/3 landscape resources, you need to configure the SAP CCMS online monitor (from the Controller) before executing the scenario, and select the statistics and measurements you want to monitor. You select these counters using the SAP CCMS dialog box.

This chapter includes:

Setting up the Monitoring Environment

Before monitoring an SAP CCMS server:

- Ensure that SiteScope has been installed on a server. You can install it on the same machine as the Controller, or on a dedicated server.
- Ensure that the SAP Java Connector (SAP JCo 2.0.6 and above) component is installed on the same server where SiteScope is running (or at least is accessible on a shared or remote location). To install the SAP Java Connector, perform the following:
  - Download the SAP Java Connector from the SAP Software Distribution Center at http://www.service.sap.com/connectors. Click **SAP Java Connector** and **Tools and Services**. You will need a valid Service Marketplace login (username and password) to access this site.
  - Follow the installation instructions that come with the SAP JCo download for your appropriate platform. On Windows, add the JCo installation location in the System Environment PATH variable. This change usually requires you to reboot Windows for the system PATH to be updated. Once completed, make the SAP JCo library file available to SiteScope by copying **sapjco.jar** (which comes with the JCo install) to **/SiteScope/java/lib/ext** before starting SiteScope.
- Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.

Note: The BC-XAL 1.0 interface is supported on SAP R/3 systems 4.5B and above only.

Adding a Machine to Monitor

In order to monitor the SAP CCMS resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the SAP CCMS graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The SAP CCMS dialog box opens.
3. In the **Monitored Server Machines** section, click **Add**. The Add Machine dialog box opens.
   - In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor, and select the platform on which the machine runs.
   - In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

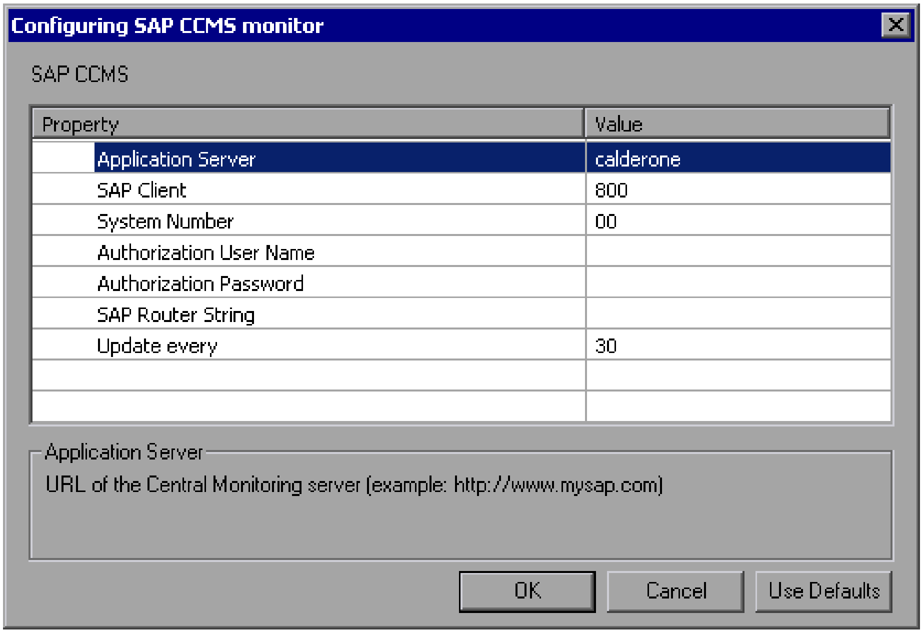
   Click **OK**. The SAP CCMS dialog box is redisplayed.
4. In the **Resource Measurements** section, click **Add**.
5. Continue with “Configuring the SAP CCMS Monitor” on page 284.

Configuring the SAP CCMS Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

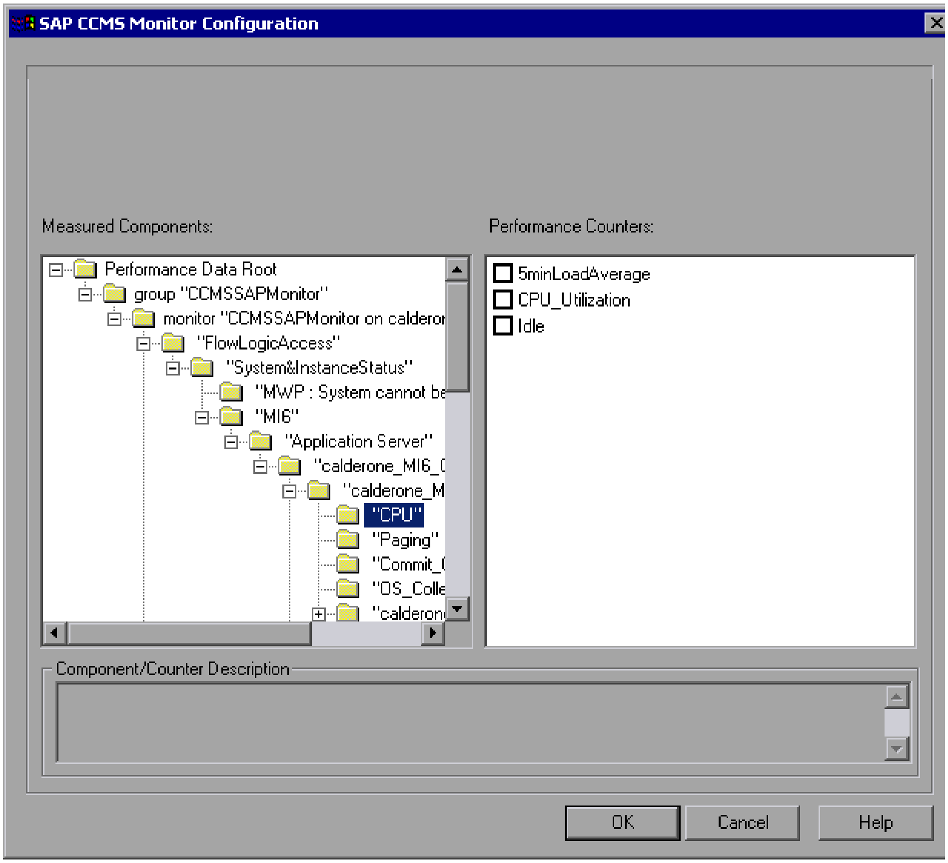
To configure the SAP CCMS monitor:

1 When you click **Add** to add a measurement, the Configuring SAP CCMS Monitor dialog box opens.



Enter the SAP CCMS configuration values, as described in “Understanding the Configuring SAP CCMS Monitor Dialog Box” on page 286.

2 Click **OK**. The SAP CCMS Monitor Configuration dialog box opens, displaying the available measurements.



Note: Due to the large amount of metrics that are retrieved, it may take several minutes to display the performance counters tree. However, once the tree has been successfully retrieved, it will be cached to a file, so that the next time you retrieve metrics from the same server and username, the wait time will be greatly reduced.

---

3 Browse the Measured Components tree, and select performance counters, as described in “Understanding the SAP CCMS Monitor Configuration Dialog Box” on page 287.

For more information on the available measurements, refer to the SAP CCMS documentation.

4 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: *<machine>* section of the SAP CCMS dialog box.

5 Click **OK** in the SAP CCMS Monitor Configuration dialog box, and in the SAP CCMS dialog box, to activate the monitor.

Note: The minimum recommended SiteScope monitor refresh rate is 30 seconds. If you choose a lower refresh rate, the Controller may not get all the data in time.

Understanding the Configuring SAP CCMS Monitor Dialog Box

The Configuring SAP CCMS Monitor dialog box enables you to configure the SAP CCMS monitor.

- **Application Server.** Enter the address of the SAP server you want to monitor.
- **SAP Client.** Enter the Client to use for connecting to SAP. A default client of 800 is typically used.
- **System Number.** Enter the System number for the SAP server. A default system number of 00 is typically used.
- **Authorization User Name.** Enter the Username required to connect to the SAP server.
- **Authorization Password.** Enter the Password required to connect to the SAP server.
- **SAP Router String.** If your connection is being made through a router, enter a router address string. You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.

- **Update every.** Enter how frequently (in seconds) the monitor should check the SAP server. SAP CCMS metrics are generally updated once every five minutes.

Understanding the SAP CCMS Monitor Configuration Dialog Box

The SAP CCMS dialog box lets you select the SAP CCMS resources to monitor.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

33

SAPGUI Server Resource Monitoring

The SAPGUI monitor displays statistics about the resource usage of an SAP R/3 system during the scenario run.

You can use the SAPGUI monitor to view:

- the number of configured instances for each SAP system
- data for all application instances (not just the one you logged on to)
- transactions used and the users that call them
- number of users working on the different instances
- performance history for recent periods of all instances
- response time distribution
- resource consumption for any application server
- application server workload for the current day or for a recent period

To obtain data on the SAP R/3 system server, you need to configure the SAPGUI online monitor (from the Controller) before executing the scenario, and indicate which statistics and measurements you want to monitor. You select these counters using the Add SAPGUI Monitor Measurements dialog box.

Note: The SAPGUI monitor supports SAP server versions 3.1 to 4.6, regardless of the SAP R/3 server's operating system and the platform on which it is installed.

This chapter includes:

Setting Up the Monitoring Environment

Before monitoring an SAP R/3 system server, perform the following:

- Install the SAPGUI for Windows 6.20 client on the Controller machine.
- Install the latest patch for the SAPGUI for Windows 6.20 client. The lowest supported level is patch 36. (SAPGUI patches can be downloaded from https://websmp104.sap-ag.de/patches. You will need a valid Service Marketplace username and password to access this site.)
- From the SAPGUI client application, press **F6** to determine whether you can access the st03 transaction and query for **last minute load** information. If this functionality is not already enabled, enable it from the SAP R/3 client on the Controller machine, using the username and password defined in the Controller.

Adding a Machine to Monitor

In order to monitor the SAPGUI resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

Limitation: Once the SAPGUI monitor is activated on the Controller machine, you cannot record a SAPGUI protocol script on that machine.

To add a machine to the Controller:

1. Click the SAPGUI graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The SAPGUI dialog box opens.
3. In the **Monitored Server Machines** section, click **Add**. The Add Machine dialog box opens.
4. Enter the logical name of the server you want to monitor, select the platform on which the machine runs, and click **OK**. To determine the logical name, see the status bar of the SAP user interface when you are connected to a server, as displayed in the figure above.

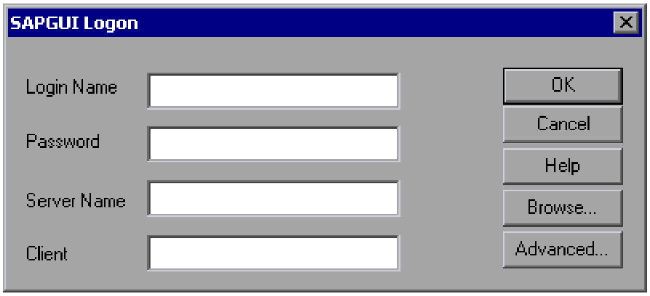
   The SAPGUI dialog box is redisplayed.
5. In the **Resource Measurements** section of the SAPGUI dialog box, click **Add**.
6. Continue with Configuring the SAPGUI Monitor below.

Configuring the SAPGUI Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the SAPGUI monitor:

1 When you click **Add** to add a measurement, the SAPGUI Logon dialog box opens.

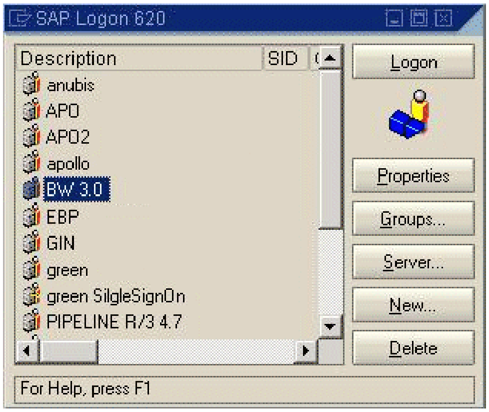


Enter the following information in the SAPGUI Logon dialog box:

- **Login Name.** Login name used to access the SAPGUI server.
- **Password.** Password for the login name.
- **Server Name.** Name of the SAPGUI server.
- **Client**. Number used in the Client field of the SAP logon details

You can enter the server name in the following ways:

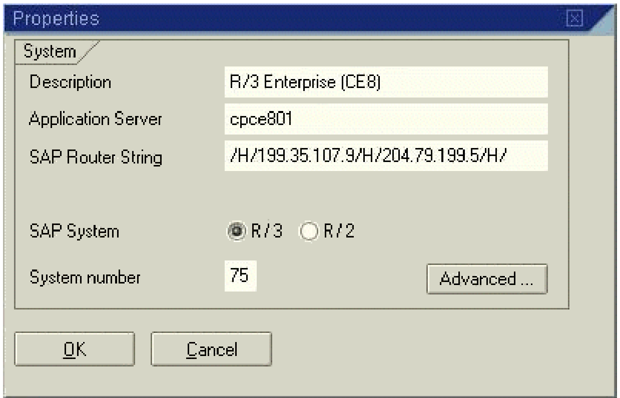
➤ The server description, as displayed in the SAP Logon application (for example BW 3.0 in the SAP Logon dialog box displayed below).



➤ A string, in the format: server_network_name[:system_number]

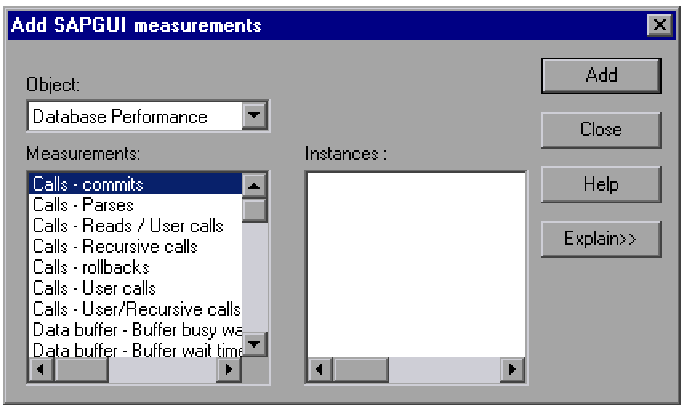
where server_network_name is the name or IP address of the application server as it is displayed in the Server Name field of the LoadRunner SAPGUI Logon dialog box (for example: pipeline.HP.com), and system_number (preceded by ":") is the system number as it is displayed in the Properties dialog box. If the system number is omitted, "00" is used by default.

If an SAP router string is also specified in the Properties dialog box, the server_network_name should be the concatenation of the router string and the application server (for example, /H/199.35.107.9/H/204.79.199.5/H/cpce801 in the Properties dialog box displayed below).



2 To change the default language, click **Advanced** in the LoadRunner SAPGUI Logon dialog box, and enter a 2-letter string in the Language field.

3 Click **OK**. The Add SAPGUI Measurements dialog box opens.



4 For each measurement, select an object, measurement, and instance, and then click **Add**, as described in "Understanding the Add SAPGUI Measurements Dialog Box" on page 295.

For a description of the available measurements, see "SAPGUI Performance Counters" on page 296.

5 Click **Add** to place the selected measurement on the resource list. Add all the desired resources to the list, and click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the SAPGUI dialog box.

6 Click **OK** in the SAPGUI dialog box to activate the monitor.

Understanding the Add SAPGUI Measurements Dialog Box

The Add SAPGUI Measurements dialog box enables you to select the SAP resources to monitor.

- **Object.** Select the object being monitored on the specified machine.
- **Measurements.** Select resource measurements to monitor. You can select multiple measurements using the CTRL key.
- **Instances.** If multiple instances of the selected measurement are running, select one or more instances to monitor for the selected measurement.
- **Add.** Click to add the selected object, measurement, and instance to the monitored measurement list.
- **Explain.** Displays a description of the selected measurement.

SAPGUI Performance Counters

The following table lists the most commonly monitored counters:

Measurement	Description
Average CPU time	The average CPU time used in the work process.
Average response time	The average response time, measured from the time a dialog sends a request to the dispatcher work process, through the processing of the dialog, until the dialog is completed and the data is passed to the presentation layer. The response time between the SAP GUI and the dispatcher is not included in this value.
Average wait time	The average amount of time that an unprocessed dialog step waits in the dispatcher queue for a free work process. Under normal conditions, the dispatcher work process should pass a dialog step to the application process immediately after receiving the request from the dialog step. Under these conditions, the average wait time would be a few milliseconds. A heavy load on the application server or on the entire system causes queues at the dispatcher queue.
Average load time	The time needed to load and generate objects, such as ABAP source code and screen information, from the database.
Database calls	The number of parsed requests sent to the database.
Database requests	The number of logical ABAP requests for data in the database. These requests are passed through the R/3 database interface and parsed into individual database calls. The proportion of database calls to database requests is important. If access to information in a table is buffered in the SAP buffers, database calls to the database server are not required. Therefore, the ratio of calls/requests gives an overall indication of the efficiency of table buffering. A good ratio would be 1:10.

Measurement	Description
Roll ins	The number of rolled-in user contexts.
Roll outs	The number of rolled-out user contexts.
Roll in time	The processing time for roll ins.
Roll out time	The processing time for roll outs.
Roll wait time	The queue time in the roll area. When synchronous RFCs are called, the work process executes a roll out and may have to wait for the end of the RFC in the roll area, even if the dialog step is not yet completed. In the roll area, RFC server programs can also wait for other RFCs sent to them.
Average time per logical DB call	The average response time for all commands sent to the database system (in milliseconds). The time depends on the CPU capacity of the database server, the network, the buffering, and on the input/output capabilities of the database server. Access times for buffered tables are many magnitudes faster and are not considered in the measurement.

34

Siebel Web Server Resource Monitoring

The Siebel Web Server monitor displays statistics about the resource usage of a Siebel Web Server during the scenario run.

To obtain data on the Siebel Web Server, you need to configure the Siebel Web Server online monitor (from the Controller) before executing the scenario, and indicate which statistics and measurements you want to monitor. You select these counters using the Siebel Web Server dialog box.

This chapter includes:

Setting up the Monitoring Environment

Before monitoring a Siebel Web Server, perform the following:

- Ensure that the Siebel Web server plug-in is installed and configured to enable the display of the statistics you want to monitor. This may require that stats page sections be enabled by editing the **eapps.cfg** file for the Siebel server. For more information, refer to the Siebel documentation.
- Ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.

Adding a Machine to Monitor

In order to monitor the Siebel Web resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the Siebel Web Server graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Siebel Web Server dialog box opens.
3. In the **Monitored Server Machines** section, click **Add**. The Add Machine dialog box opens.

   ➤ In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor, and select the platform on which the machine runs.

   ➤ In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

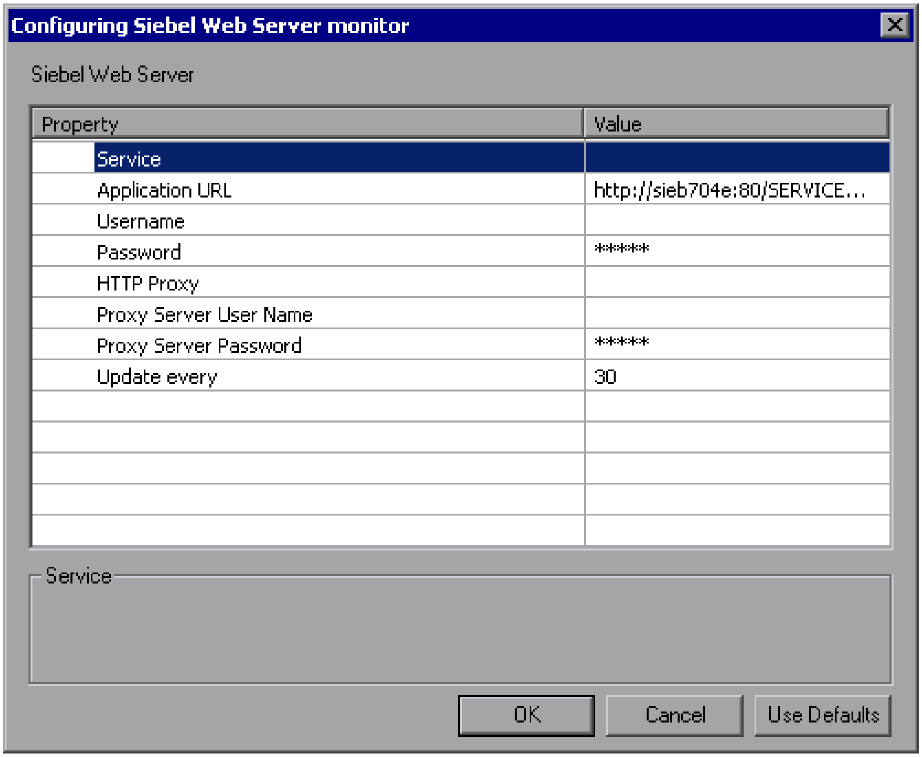
   Click **OK**. The Siebel Web Server dialog box is redisplayed.
4. In the **Resource Measurements** section of the Siebel Web Server dialog box, click **Add**.
5. Continue with “Configuring the Siebel Web Server Monitor” on page 301.

Configuring the Siebel Web Server Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

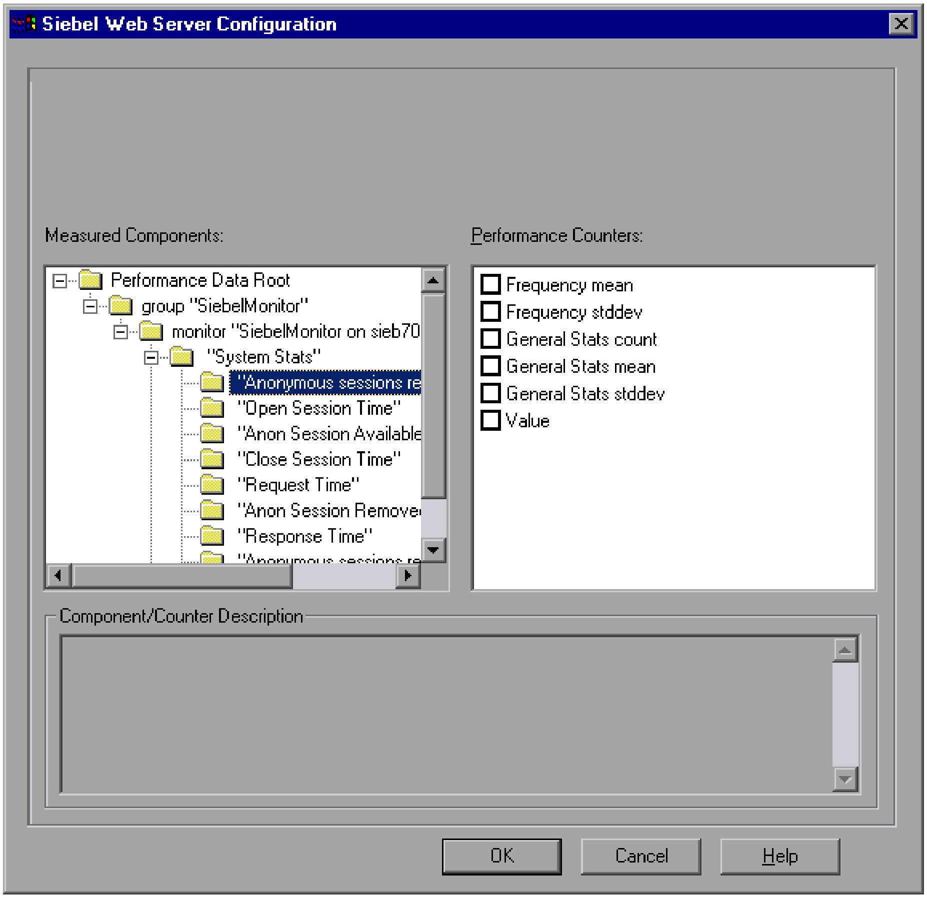
To configure the Siebel Web Server monitor:

1 When you click **Add** to add a measurement, the Configuring Siebel Web Server Monitor dialog box opens.



Enter the Siebel Web Server information, as described in "Understanding the Configuring Siebel Web Server Monitor Dialog Box" on page 303.

2 Click **OK**. The Siebel Web Server Configuration dialog box opens, displaying the available measurements.



3 Browse the Measured Components tree, and select performance counters, as described in "Understanding the Siebel Web Server Configuration Dialog Box" on page 304.

For a description of the available measurements, see "Siebel Web Server Performance Counters" on page 305.

4 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the Siebel Web Server dialog box.

5 Click **OK** in the Siebel Web Server dialog box, to activate the monitor.

Note: The minimum recommended SiteScope monitor refresh rate is 30 seconds. If you choose a lower refresh rate, the Controller may not get all the data in time.

Understanding the Configuring Siebel Web Server Monitor Dialog Box

The Configuring Siebel Web Server Monitor dialog box enables you to configure the Siebel Web Server monitor.

- **Service.** Enter the name of a valid Siebel virtual directory (for example, callcenter or sales), one whose URL is an entry point defined in the Siebel SWSE configuration file (eapps.cfg).
- **Application URL.** Displays the default URL of the web plug-in server stats page for the application you want to monitor.

  For example, http://siebelsrv/<service>/_stats.swe.

  If the Siebel web server is configured to support verbose mode, and you want to include information on "Locks" and "Current Operations Processing," you can add verbose=high.

  For example: http://siebelsrv/<service>/_stats.swe?verbose=high.
- **Username.** Enter the user name to access the web server stats page.
- **Password.** Enter the password to accessing the web server stats page.
- **HTTP Proxy.** If you are using a proxy to access the Siebel server, enter the proxy server to use including the port (for example, **proxy.sitescope.com:8080**).
- **Proxy Server User Name.** If the proxy server requires authorization, enter the proxy user name.
- **Proxy Server Password.** If the proxy server requires authorization, enter the proxy password.
- **Update every.** Enter how frequently the monitor should check the Database server.

Understanding the Siebel Web Server Configuration Dialog Box

The Siebel Web Server Configuration dialog box lets you select the Siebel Web Server resources to monitor.

- **Host.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

Siebel Web Server Performance Counters

The following tables shows the default counters that can be measured:

System Statistics

Measurement	Description
Anonymous sessions requested from the pool	The number of anonymous sessions requested from the pool.
Open Session Time	The time taken for users to log on to the system.
Anon Session Available	The number of anonymous sessions available in the pool.
Close Session Time	The time taken for users to log off the system.
Request Time	The time taken to process the user request.
Anon Session Removed	The number of anonymous sessions removed from the pool.
Response Time	The time taken to respond to a user request.
Anonymous sessions returns to the pool	The number of anonymous sessions returned to the pool.

Application Statistics

Measurement	Description
Session Lifespan	The duration during which a client session ran in the Siebel system.

35

Siebel Server Manager Resource Monitoring

The Siebel Server Manager monitor displays statistics about the resource usage of a Siebel Server Manager during the scenario run.

To monitor Siebel Server Manager performance, you first install the Siebel Server Manager client on the SiteScope machine. You must then enable the Siebel Server Manager online monitor (from the Controller) before executing the scenario, and indicate which statistics and measurements you want to monitor. You select these counters using the Siebel Server Manager dialog box.

This chapter includes:

Setting up the Monitoring Environment

Before you set up the monitor, perform the following:

- Ensure that SiteScope has been installed on a server. You can install it on the Controller, or on a dedicated server. If SiteScope is installed on a machine other than the Controller, verify that the SiteScope machine is accessible from the Controller machine.
- On the machine where SiteScope is installed, configure SiteScope to monitor the required Siebel Server Manager machine. For more information, see "Configuring the Siebel Server Manager Client on the SiteScope Machine" on page 308.
- Verify that SiteScope is collecting the required data from the servers it is monitoring. From the SiteScope Panel, select the monitor group polling the Siebel Server Manager machine, and check that the monitor displays a list of server measurements in the Status column.

Configuring the Siebel Server Manager Client on the SiteScope Machine

1. Verify connectivity to the Siebel SWSE page by opening the following URL from the machine where Sitescope is installed:

   http://<your_siebel_server>/callcenter/_stats.swe

2. In the SiteScope main panel, select an existing group or create a new group.
3. In the **Add to Group** section, click **Monitor** and select **Siebel Server Manager** from the list of monitors.
4. Click **Choose server**, and enter the name of the Siebel Server in the **Application server** field, the Enterprise Server in the **Enterprise server** field, and the Gateway Server in the **Gateway server** field.
5. If necessary, enter the user name and password for the Siebel Server Manager client.
6. Enter the path to the Siebel Server Manager in the **Path to Script** field.
7. Click **Browse**, select your desired counters, and then click **Choose** Counters.

8 In the **Title** field, enter a name for the monitor.

Note: When you assign a name to a monitor, include the server name in the monitor name. This avoids any confusion as to which host the monitor belongs. For example, SiebelManager on sieb07.

Do not use "\" in the Title field.

---

9 Click **Add Monitor**.

Troubleshooting the Siebel Server Manager Monitor

The Siebel Server Manager monitor uses a Siebel command line utility (srvrmgr) to gather it's statistics. If you are having trouble getting the Siebel Server Manager monitor to work, run this command from the Siebel Server Manager client:

```
srvrmgr /s <server> /g <gateway> /e <enterprise> /u <user> /p <pw>
```

If this command works from the command line, but SiteScope has trouble executing the command, open **/sitescope/templates.applications/commandline.siebel,** and verify that you can run the following command from the command line:

```
CONNECT_COMMAND:$PATH$/srvrmgr /g $GATEWAY$ /e $ENTERPRISE$
/s $SERVERS$ /u $USERNAME$ /p $PASSWORD$
```

Note: On a Windows 2000 Advanced Server platform this command must be changed to:

```
CONNECT_COMMAND:$PATH$\srvrmgr.exe /g $GATEWAY$ /e
$ENTERPRISE$ /s $SERVERS$ /u $USERNAME$ /p $PASSWORD$
```

Adding a Machine to Monitor

In order to monitor the Siebel Server Manager resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

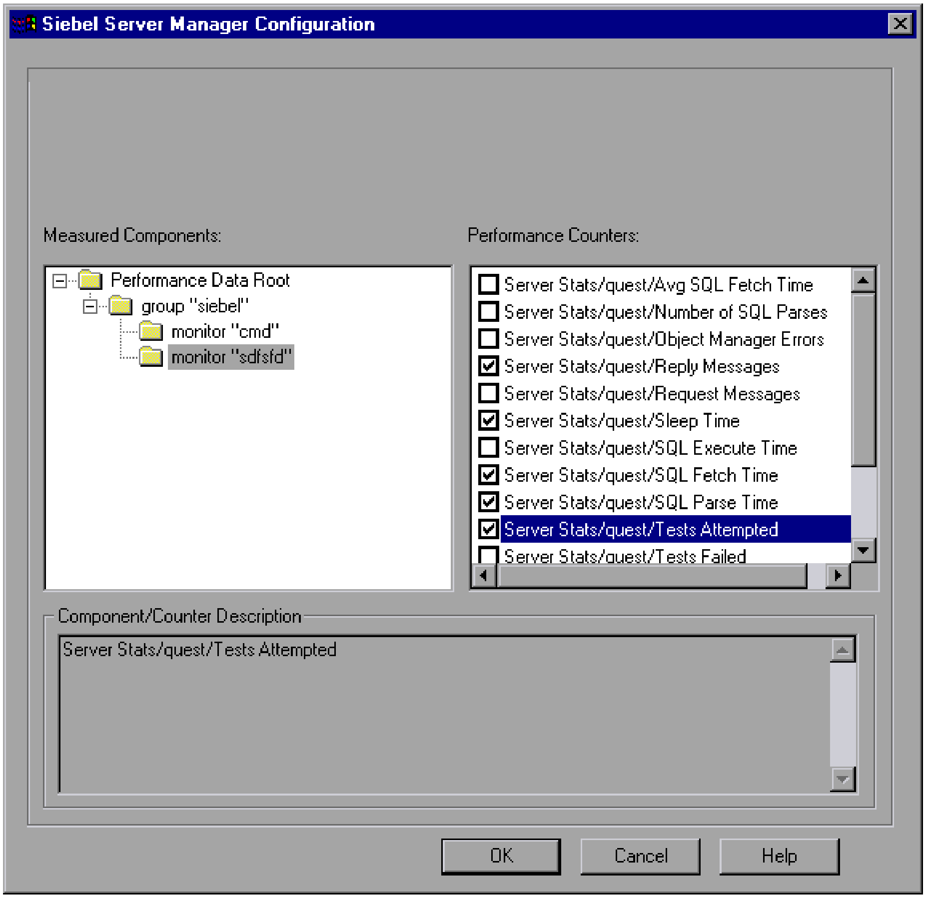
1. Click the Siebel Server Manager graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Siebel Server Manager dialog box opens.
3. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
4. Enter the server name or IP address of the machine you want to monitor, select the platform on which the machine runs, and click **OK**. The Siebel Sever Manager dialog box is redisplayed.
5. In the **Resource Measurements** section of the Siebel Server Manager dialog box, click **Add.**
6. Continue with Configuring the Siebel Server Manager Monitor below.

Configuring the Siebel Server Manager Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the Siebel Server Manager monitor:

1 When you click **Add** to add a measurement, the Siebel Server Manager Configuration dialog box opens, displaying the available measurements.



2 Browse the Measured Components tree, select the required performance counters, as described in "Understanding the Siebel Server Manager Configuration Dialog Box" on page 312.

For a description of the available measurements, see "Siebel Server Manager Performance Counters" on page 313.

3 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the Siebel Server Manager dialog box.

4 Click **OK** in the Siebel Server Manager dialog box to activate the monitor.

Note: The minimum recommended SiteScope monitor refresh rate is 30 seconds. If you choose a lower refresh rate, the Controller may not get all the data in time.

Limitations

The SiteScope monitor has the following limitations when it retrieves information from a Siebel Server Manager:

- The component counters (for example, Average SQL Time for <component>) are updated with the aggregated Siebel data only at the end of a user session.
- The SiteScope monitor consumes very high CPU resources (approximately 40%).

Understanding the Siebel Server Manager Configuration Dialog Box

The Siebel Server Manager Configuration dialog box enables you to select the Siebel Server Manager resources to monitor.

- **Host.** Displays the name of the monitored machine.

- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Select performance counters.
- **Component/Counter Description.** Displays a description of the selected component or counter.

Siebel Server Manager Performance Counters

The following table shows the default counters that can be measured:

Measurement	Description
Average Connect Time	The average connection time.
Average Reply Size	The average size of a user reply.
Average Request Size	The average size of a user request.
Average Requests Per Session	The average number of user requests per session.
Average Response Time	The average amount of time that it takes the server to respond to a request.
Average Think Time	The average amount of think time taken to respond to a request.
Avg SQL Execute Time	The average SQL execute time.
Avg SQL Fetch Time	The average SQL fetch time.
Avg SQL Parse Time	The average SQL parse time.
CPU Time	The CPU time used in the work process.
Elapsed Time	The total amount of elapsed time.
Num of DBConn Retries	The number of database connection retries.
Num of DLRbk Retries	The number of DLRbk retries.

Measurement	Description
Num of Exhausted Retries	The total number of retries that expired.
Number of SQL Executes	The total number of SQL executes.
Number of SQL Fetches	The total number of SQL fetches.
Number of SQL Parses	The total number of SQL parses.
Number of Sleeps	The number of sleeps.
Object Manager Errors	The total number of object manager errors.
Reply Messages	The total number of reply messages.
Request Messages	The total number of request messages.
SQL Execute Time	The total SQL execute time.
SQL Fetch Time	The total SQL fetch time.
SQL Parse Time	The total SQL parse time.
Sleep Time	The total sleep time.
Tests Attempted	The number of tests attempted.
Tests Failed	The number of tests that failed.
Tests Successful	The number of tests that were successful.
Total Reply Size	The total reply size, measured in bytes.
Total Request Size	The total request size, measured in bytes.
Total Response Time	The total response time.
Total Tasks	The total number of tasks.
Total Think Time	The total think time.

36

PeopleSoft (Tuxedo) Resource Monitoring

The PeopleSoft (Tuxedo) monitor displays statistics about the resource usage of a PeopleSoft (Tuxedo) server during the scenario run.

To obtain data for this graph, you need to configure the PeopleSoft (Tuxedo) online monitor (from the Controller) and select the measurements you want to display, before running the scenario. You select these counters using the PeopleSoft (Tuxedo) dialog box.

This chapter includes:

Setting up the Monitoring Environment

If Tuxedo 7.1 or later is installed, you can monitor more than one PeopleSoft (Tuxedo) application server at a time. If Tuxedo 6.5 or earlier is installed, you can monitor only one PeopleSoft (Tuxedo) application server at a time.

Before you set up the monitor, perform the following:

- Ensure that a Tuxedo workstation client (not a native client), version 6.3 or later, is installed on the Controller machine. Use a Tuxedo 6.x client if a Tuxedo 6.x server is used, and Tuxedo 7.1 or later client if a Tuxedo 7.1 or later server is used. If you use a Tuxedo 6.5 or earlier server, you can still use a Tuxedo 7.1 or later client in order to monitor it, provided that you set the WSINTOPPRE71 environment variable to “yes”.

Note: A Tuxedo workstation client communicates with the application server over the network, and is not required to run the Tuxedo application server on the same machine. A native client can only communicate with the Tuxedo application server if it is part of the relevant Tuxedo domain.

- Define the Tuxedo environment variables on the Controller machine—set the TUXDIR variable to the Tuxedo installation directory (for example, V:\environ\32\Tuxedo 8.0), and add the Tuxedo **bin** directory to the PATH variable.
- Ensure that the workstation listener (WSL) process is running. This enables the application server to accept requests from workstation clients. The address and port number used to connect to the application server must match those dedicated to the WSL process.

Note: For information on configuring the WSL, refer to the BEA Tuxedo Web site (http://edocs.beasys.com/tuxedo/tux81/rf5/rf5101.htm#1534543).

Adding a Machine to Monitor

In order to monitor the PeopleSoft (Tuxedo) resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the PeopleSoft (Tuxedo) graph in the graph tree, and drag it into the right pane of the **Run** view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Online Measurement**. The PeopleSoft (Tuxedo) dialog box opens.
3. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

4 Enter the server name or IP address of the Tuxedo machine you want to monitor.

Note: If you are using multiple instances of the PeopleSoft (Tuxedo) monitor on the same machine, then enter the port number of PeopleSoft (Tuxedo) monitor in order to distinguish one instance from another. The entry should have the following format: <machine name>:<port number>

Select the platform on which the machine runs, and click **OK**.

5 In the **Resource Measurements** section of the PeopleSoft (Tuxedo) dialog box, click **Add**.

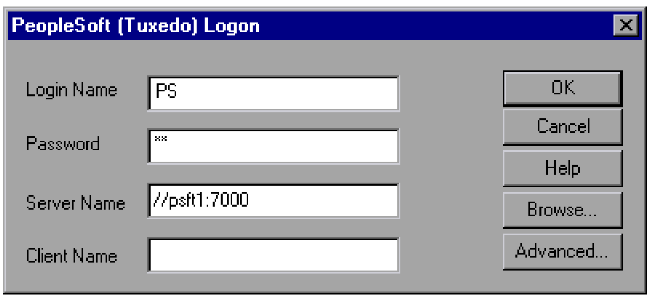
6 Continue with Configuring the PeopleSoft (Tuxedo) Monitor below.

Configuring the PeopleSoft (Tuxedo) Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the PeopleSoft (Tuxedo) monitor:

1 When you click **Add** to add a measurement, the PeopleSoft (Tuxedo) Logon dialog box opens.



Enter the following information:

- **Login Name.** Enter the login name used to access the PeopleSoft (Tuxedo) server. The default is PS.
- **Password.** Enter the password for the login name. The default is PS.
- **Server Name.** Enter the name of the PeopleSoft (Tuxedo) server in the format of //<machine name>:<port number>. The default port is 7000. Alternatively, you can specify the IP address or the hexadecimal format used by old versions of Tuxedo.

  Note: You cannot use quotation marks.
- **Client.** Enter the name of the client machine.

Note: If you are using PeopleSoft 7.x, you can determine the logon information from the **Logon** section of the **tpinit.ini** file in the recorded script's directory.

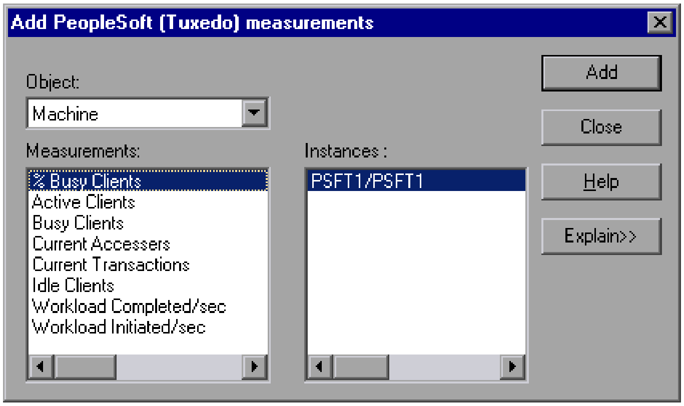
---

2 To authenticate the PeopleSoft (Tuxedo) monitor, click **Advanced**, and enter the authentication data as a hexadecimal string (beginning with "0x") in the **Data** field. The authentication data value can be obtained from the **tpinit.ini** file of an existing Tuxedo script.

Note: If you are using Tuxedo 6.5 or below, the monitor can only connect to one application server during a Controller scenario. Once it connects to an application server, that server is the only one used by the monitor until the Controller is closed. This applies even when all of the counters are deleted from the monitor.

---

3 Click **OK**. The Add PeopleSoft (Tuxedo) Measurements dialog box opens.



4 For each measurement, select an object, measurement, and instance, and then click **Add**, as described in “Understanding the Add PeopleSoft (Tuxedo) Measurements Dialog Box” on page 320.

For a description of the available measurements, see “PeopleSoft (Tuxedo) Performance Counters” on page 320.

5 When you have finished adding measurements, click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the PeopleSoft (Tuxedo) dialog box.

6 Click **OK** in the PeopleSoft (Tuxedo) dialog box to activate the monitor.

Understanding the Add PeopleSoft (Tuxedo) Measurements Dialog Box

The Add PeopleSoft (Tuxedo) Measurements dialog box enables you to select the PeopleSoft (Tuxedo) resources to monitor.

- **Object.** Select the object being monitored on the specified machine.
- **Measurements.** Select a resource measurement to monitor. Select multiple measurements using the CTRL key. For an explanation of each measurement, click **Explain**.
- **Instances.** If multiple instances of the selected measurement are running, select one or more instances to monitor for the selected measurement.
- **Explain.** Displays a description of the selected measurement.

PeopleSoft (Tuxedo) Performance Counters

The following table describes the default counters that can be measured. It is recommended to pay particular attention to the following measurements: % Busy Clients, Active Clients, Busy Clients, Idle Clients, and all the queue counters for the APPQ/PSAPPSRV queue.

Monitor	Measurements
Machine	**% Busy Clients** - The percent of active clients currently logged in to the Tuxedo application server that are waiting for a response from the application server.
	Active Clients - The total number of active clients currently logged in to the Tuxedo application server.
	Busy Clients - The total number of active clients currently logged in to the Tuxedo application server that are waiting for a response from the application server.
	Current Accessers - The number of clients and servers currently accessing the application either directly on this machine or through a workstation handler on this machine.
	Current Transactions - The number of in use transaction table entries on this machine.
	Idle Clients - The total number of active clients currently logged in to the Tuxedo application server that are not waiting for a response from the application server.
	Workload Completed/second - The total workload on all the servers for the machine that was completed, per unit time.
	Workload Initiated/second - The total workload on all the servers for the machine that was initiated, per unit time.

Monitor	Measurements
Queue	**% Busy Servers** - The percent of active servers currently handling Tuxedo requests.
	Active Servers - The total number of active servers either handling or waiting to handle Tuxedo requests.
	Busy Servers - The total number of active servers currently busy handling Tuxedo requests.
	Idle Servers - The total number of active servers currently waiting to handle Tuxedo requests.
	Number Queued - The total number of messages which have been placed on the queue.
Server	**Requests/second** - The number of server requests handled per second.
	Workload/second -The workload is a weighted measure of the server requests. Some requests could have a different weight than others. By default, the workload is always 50 times the number of requests.
Workstation Handler (WSH)	**Bytes Received/sec** - The total number of bytes received by the workstation handler, per second.
	Bytes Sent/sec - The total number of bytes sent back to the clients by the workstation handler, per second.
	Messages Received/sec - The number of messages received by the workstation handler, per second.
	Messages Sent/sec - The number of messages sent back to the clients by the workstation handler, per second.
	Number of Queue Blocks/sec - The number of times the queue for the workstation handler blocked, per second. This gives an idea of how often the workstation handler was overloaded.

Part XII

Application Component Monitoring

37

Introduction to Application Component Monitoring

Using LoadRunner's Application Component monitors, you can monitor the Microsoft COM+ server during a scenario run in order to isolate server performance bottlenecks.

Application Component monitors provide you with information about the resource usage of the Microsoft COM+ server during scenario execution. In order to obtain this data, you need to activate the online monitor for the server and specify which resources you want to measure before executing the scenario.

38

Microsoft COM+ Server Monitoring

The Microsoft COM+ monitor is an Application Component monitor that provides performance information for the Microsoft COM+ server. Before monitoring a Microsoft COM+ server, you install the Microsoft COM+ Server Monitor Probe on the server machine. You can then specify which measurements and resources you want the Microsoft COM+ monitor to measure. You select these counters using the Controller's monitor configuration dialog box.

This chapter includes:

Setting up the Monitoring Environment

To monitor the Microsoft COM+ server performance, you must first install the Microsoft COM+ Server Monitor Probe on the server machine. You can then specify which measurements and resources you want the Microsoft COM+ monitor to measure. You select these counters using the Controller's monitor configuration dialog box.

For more information on installing the Microsoft COM+ server add-in, refer to the *HP LoadRunner Installation Guide*.

Adding and Configuring a Machine to Monitor

In order to monitor the MS-COM+ resources of a particular machine you need to add the machine, and add the measurements that you want to monitor.

You select measurements to monitor the COM+ server using the Microsoft COM+ Performance Monitors dialog box.

To add the MS-COM+ monitor:

1 Click the Microsoft COM+ graph in the graph tree, and drag it into the right pane of the Run view.

2 Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Microsoft COM+ dialog box opens.

   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

   For regular monitoring without a firewall, enter the server name or IP address of the machine you want to monitor, select the platform on which the machine runs, and click **OK**.

3 To connect to the monitor over a firewall, enter the server name or IP address of the machine you want to monitor, according to the following format, and click **OK**:

   ```
   <MI Listener machine>:<server machine key>
   ```

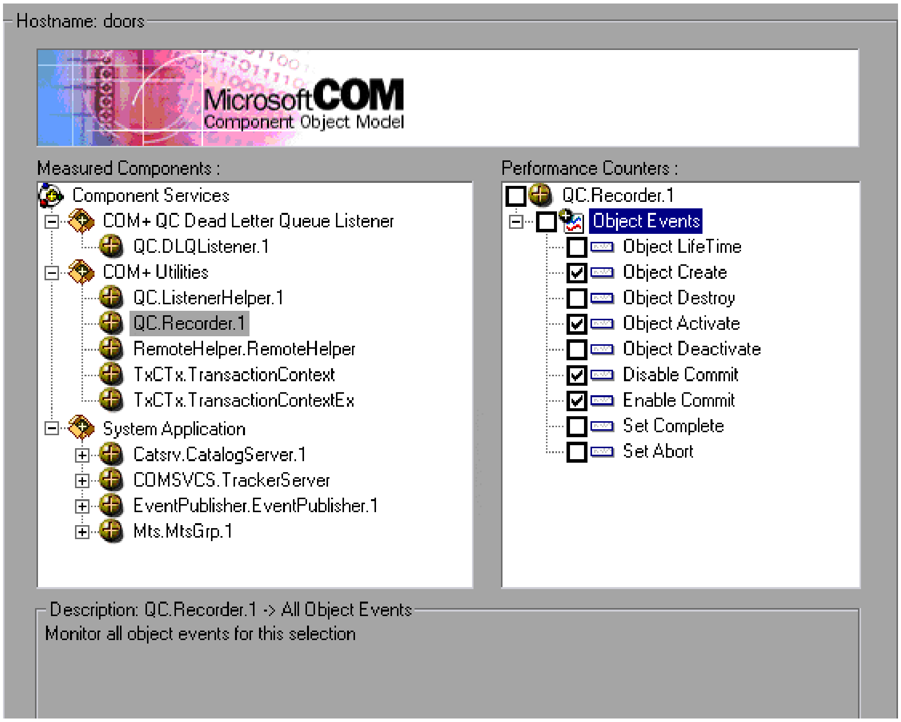
   where **server machine key** is the unique key that you chose when configuring the firewall Agent on the server machine.

   For example: `12.12.12.3:serverid`

To configure the MS-COM+ monitor:

1 In the **Resource Measurements section** of the Microsoft COM+ dialog box, click **Add** to select the measurements that you want to monitor.

The Microsoft COM+ Monitors Configuration dialog box opens displaying the available measurements.



2 Browse the Measured Components tree, and check the required performance counters, as described in "Understanding the COM+ Monitor Configuration Dialog Box" on page 330.

For a description of the available measurements, see "Microsoft COM+ Performance Counters" on page 331.

3 Click **OK**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the Microsoft COM+ dialog box.

4 Click **OK** in the Microsoft COM+ dialog box to activate the Microsoft COM+ monitor.

Note: The data sampling rate for the COM+ monitor is fixed and cannot be modified using the Controller **Tools** > **Options**> **Monitors** dialog.

Understanding the COM+ Monitor Configuration Dialog Box

The Microsoft COM+ Monitors Configuration dialog box lets you select the items to monitor on the Microsoft COM+ server.

- **Hostname.** Displays the name of the monitored machine.
- **Measured Components.** Displays the available components. Browse the tree and select the component you want to monitor. A description of the highlighted component appears in the Component/Counter Description box.
- **Performance Counters.** Check the required performance counters. A description of the selected counter appears in the Component/Counter Description box.
- **Component/Counter Description.** Displays a description of the selected component or counter.

Configuring the Microsoft COM+ Monitor Over a Firewall

Before running the Microsoft COM+ Monitor over a firewall:

- Make sure that the MI Listener is installed on any machine (including the Controller machine) outside of the firewall. Refer to the *HP LoadRunner Installation Guide* for installation instructions.
- Configure the firewall agent on the server machine. For more information, refer to the chapter called "Working with Firewalls in LoadRunner", in the *HP LoadRunner Controller User Guide*.
- Specify the correct connection string on the client machine, as described in step 3 of "Adding and Configuring a Machine to Monitor" on page 328.

Microsoft COM+ Performance Counters

The following tables describe the default counters that can be measured:

Authentication Metrics

Measurement	Description
Authenticate	Frequency of successful method call level authentication. When you set an authentication level for an application, you determine what degree of authentication is performed when clients call into the application.
Authenticate Failed	Frequency of failed method call level authentication.

Application Events

Measurement	Description
Activation	Frequency of application activation or startup.
Shutdown	Frequency of application shutdown or termination.

Thread Events

Measurement	Description
Thread Start	Rate at which single-threaded apartment (STA) thread for application have been started.
Thread Terminate	Rate at which single-threaded apartment (STA) thread for application have been terminated.
Work Enque	Event sent if a work is queued in single thread apartment object (STA). Note: These events are not signaled/sent in Windows Server 2003 and later.
Work Reject	Event sent if a work is rejected from single thread apartment object (STA). Note: These events are not signaled/sent in Windows Server 2003 and later.

Transaction Events

Measurement	Description
Transaction Duration	Duration of COM+ transactions for selected application.
Transaction Start	Rate at which transactions have started.
Transaction Prepared	Rate at which transactions have completed the prepare phase of the two-phase protocol.
Transaction Aborted	Rate at which transactions have been aborted.
Transaction Commit	Rate at which transactions have completed the commit protocol.

Object Events

Measurement	Description
Object Life Time	Duration of object existence (from instantiation to destruction).
Object Create	Rate at which new instances of this object are created.
Object Destroy	Rate at which instances of the object are destroyed.
Object Activate	Rate of retrieving instances of a new JIT-activated object.
Object Deactivation	Rate of freeing JIT-activated object via SetComplete or SetAbort.
Disable Commit	Rate of client calls to DisableCommit on a context. DisableCommit declares that the object's transactional updates are inconsistent and can't be committed in their present state.
Enable Commit	Rate of client calls to EnableCommit on a context. EnableCommit declares that the current object's work is not necessarily finished, but that its transactional updates are consistent and could be committed in their present form.
Set Complete	Rate of client calls to SetComplete on a context. SetComplete declares that the transaction in which the object is executing can be committed, and that the object should be deactivated on returning from the currently executing method call.
Set Abort	Rate of client calls to SetAbort on a context. SetAbort declares that the transaction in which the object is executing must be aborted, and that the object should be deactivated on returning from the currently executing method call.

Method Events

Measurement	Description
Method Duration	Average duration of method.
Method Frequency	Frequency of method invocation.
Method Failed	Frequency of failed methods (i.e. methods that return error HRESULT codes).
Method Exceptions	Frequency of exceptions thrown by selected method.

Part XIII

Application Deployment Monitoring

39

Introduction to Application Deployment Solution Monitoring

Using LoadRunner's Application Deployment Solution monitor, you can isolate server performance bottlenecks by monitoring the Citrix MetaFrame XP server during a scenario run.

LoadRunner's Citrix MetaFrame XP monitor provides you with information about the application deployment usage of the Citrix MetaFrame XP server during a scenario execution. The Citrix Monitor allows you to monitor the server performance statistics from Citrix MetaFrame Servers. You can monitor multiple parameters (counters) with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning.

To obtain performance data, you need to activate the online monitor for the server and specify which resources you want to measure before executing the scenario.

40

Citrix MetaFrame XP Monitoring

The Citrix MetaFrame XP monitor displays statistics about the resource usage on the Citrix MetaFrame XP server machine during the scenario run.

This chapter includes:

Setting up the Monitoring Environment

➤ If you are using the SiteScope monitor engine, ensure that SiteScope has been installed on a server. You can install SiteScope on the same machine as the Controller, or on a dedicated server.

➤ To obtain data for this graph, you need to activate the Citrix MetaFrame XP monitor on the application server machine before executing the scenario, enable the counters you want to monitor on the Citrix server, and specify which measurements and resources you want the Citrix monitor to measure.

Note: The port you use to monitor a Citrix MetaFrame server through a firewall depends on the configuration of your server.

Before setting up the Citrix MetaFrame Server monitor:

1. Make sure that Citrix MetaFrame Server has been installed and is running on a computer. If the computer running Citrix MetaFrame Server is running Windows 2000, make sure that the Remote Registry service is running on it.
2. Make sure that the computer on which you are running LoadRunner has administrator privileges on the machine running Citrix.
3. From the Controller machine, map a network drive to the Citrix server machine. This ensures that the required authentication is provided to the Controller to access the resource counters.
4. Launch PerfMon from the Controller machine to enable the counters on the Citrix server. This allows you to monitor the same counters for the ICA Session object on the Citrix monitor.
5. You can configure the Citrix monitor to view ICA Session object counters only if at least one session is being run on the Citrix server. If no "real" user has opened a connection with the Citrix server, you need to first initialize or run a Citrix Vuser against the server, and only then configure the Citrix Monitor and add the ICA Session counters. If you configure the Citrix monitor without first initializing or running a Citrix Vuser (or connecting to the Citrix server as a "real" user), you will not be able to view the ICA Session object.

Note: Measurements that monitor instances are valid for the currently running Citrix session only. If you run this scenario again, you will need to reconfigure the measurements that are instance-oriented.

To monitor the different instances, ensure that the server login and logout procedures are recorded in the **Vuser_init** and **Vuser_end** sections respectively, and not in the Action section of the script. For more information, see the *HP Virtual User Generator User Guide*.

Adding a Machine to Monitor

In order to monitor the Citrix resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click **Citrix MetaFrame XP** in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on graph and choose **Monitors** > **Add Measurements**. The Citrix MetaFrame XP dialog box opens.
3. By default, LoadRunner monitors Citrix MetaFrame XP resources using the native LoadRunner monitor engine.

   If you want to monitor the Citrix MetaFrame XP resources using a SiteScope monitor, click **Advanced**.

   In the Choose Monitor Engine dialog box, choose **SiteScope**, and click **OK** to close the Monitor Engine dialog box.
4. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.

   ➤ In the **Monitored Machine Information** section, enter the server name or IP address of the machine you want to monitor. Select the platform on which the machine runs.

   ➤ In the **SiteScope Server Information** section, enter the SiteScope machine name, and port (default: 8888), and specify whether you are using a Secure HTTP connection. If you are using a SiteScope account, fill in the relevant account information.

   Note: If you are adding a native LoadRunner monitor, the **SiteScope Server Information** section does not appear.

   Click **OK** to close the Add Machine dialog box.
5. Click **Add** in the **Resource Measurements on:** <*machine*> section of the Citrix MetaFrame XP dialog box
6. Continue with Configuring the Citrix MetaFrame XP Monitor below.

Configuring the Citrix MetaFrame XP Monitor

The configuration for this monitor differs slightly depending on whether you are adding a SiteScope or native LoadRunner monitor.

This section describes:

- ➤ Configuring the Native LoadRunner Citrix MetaFrame XP Monitor
- ➤ Configuring the SiteScope Citrix MetaFrame XP Monitor

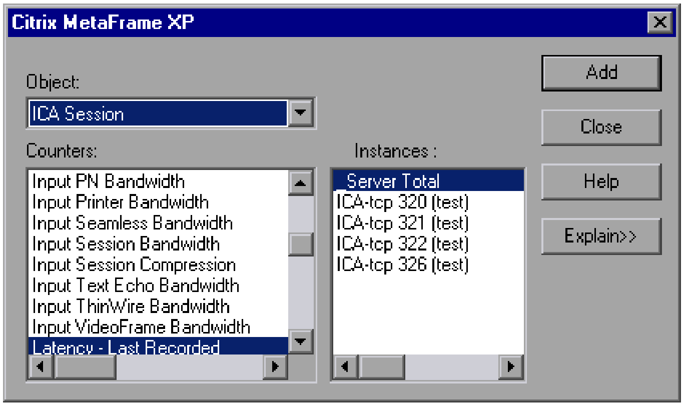
Configuring the Native LoadRunner Citrix MetaFrame XP Monitor

1 When you add a machine in the Citrix MetaFrame XP dialog box, the default measurements are displayed in the **Resource Measurements on:** <*machine*> section.

Note: To change the default counters for the Citrix monitor, see “Changing a Monitor’s Default Counters” on page 395.

- ➤ To delete a measurement from the default list, select the measurement and click **Delete**.
- ➤ To select additional measurements, click **Add**.

2 When you click **Add**, the Citrix MetaFrame XP dialog box opens displaying the Citrix resources.



For each measurement, select an object, counter, and instance, and then click **Add**, as described in "Understanding the Citrix MetaFrame XP Dialog Box" on page 344.

For a description of the available measurements, see "Citrix MetaFrame Performance Counters" on page 346.

Note: If the dialog box freezes after clicking **Add**, you may need to rebuild the localhost cache on the Citrix server machine. For more information, refer to Document IDs CTX003648 and CTX759510 in the Citrix Knowledge Base (http://knowledgebase.citrix.com/cgi-bin/webcgi.exe?New,KB=CitrixKB).

---

3 When you have finished selecting the measurements to monitor, click **Close**. The counters that you selected appear in the **Resource Measurements on**: <*machine*> section of the Citrix MetaFrame XP dialog box.

4 Click **OK** in the Citrix MetaFrame XP dialog box to activate the monitor.

Understanding the Citrix MetaFrame XP Dialog Box

The Citrix MetaFrame XP dialog box lets you select the items to monitor on the Citrix MetaFrame XP server.

- **Object.** Select the object being monitored on the specified machine.
- **Counters.** Select a resource counter to monitor. Select multiple counters using the CTRL key. For a definition of each counter, click **Explain**.
- **Instances.** If multiple instances of the selected counter are running, select one or more instances to monitor for the selected counter.
- **Add.** Click **Add** to add the measurement that you selected. The measurement is added to the list of measurements in the **Resource Measurements on.** <*machine*> section of the Citrix MetaFrame XP dialog box.
- **Explain.** Displays a definition of the selected counter.

Configuring the SiteScope Citrix MetaFrame XP Monitor

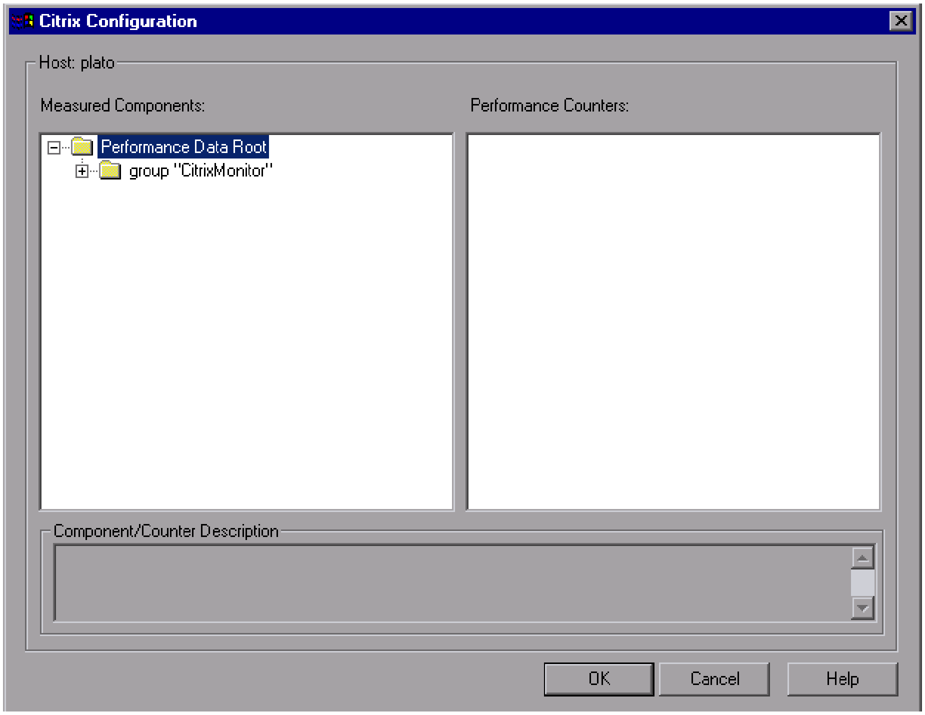
1 The first time you add measurements you need to configure the remote machine properties. When you click **Add** in the **Resource Measurements on:** <*machine*> section of the Citrix MetaFrame XP dialog box, a dialog box opens to configure the remote machine as follows:

- If you are monitoring a machine on a UNIX platform, the Configuring UNIX Remote Machine dialog box opens.
- If you are monitoring a machine on a Windows platform, the Configuring NT Remote Machine dialog box opens.

Enter the remote machine's configuration information, as described in "Configuring the Remote Machine for SiteScope Monitors" on page 25, and click **OK**.

2 The Configuring Citrix Server dialog box opens. Verify the **Server** and **Update every** properties, and click **OK**.

3 The Citrix Configuration dialog box opens, displaying the **Measured Components** list.



For each measured component select the performance counters you want to monitor, as described in "Understanding the Citrix Configuration Dialog Box" on page 346.

For a description of the available measurements, see "Citrix MetaFrame Performance Counters" on page 346.

4 When you have finished selecting the measurements to monitor, click **OK**. The counters that you selected appear in the **Resource Measurements on**: <*machine*> section of the Citrix MetaFrame XP dialog box.

5 Click **OK** to activate the monitor.

Understanding the Citrix Configuration Dialog Box

The Citrix Configuration dialog box enables you to select the performance counters to monitor using the Citrix MetaFrame XP monitor.

- **Host.** The name of the host machine.
- **Measured Components.** Displays a tree containing all the available measured components.
- **Performance Counters.** Displays the performance counters for a selected measured component.
- **Component/Counter Description.** Displays a description of the selected measured component or performance counter.

Citrix MetaFrame Performance Counters

The following table describes some of the counters that can be measured.

Non-Virtual Counters

The following table describes non-virtual counters:

Measurement	Description
% Disk Time	The percentage of elapsed time that the selected disk drive services read or write requests.
% Processor Time	The percentage of time that the processor executes a non-Idle thread. This counter is a primary indicator of processor activity. It is calculated by measuring the time that the processor spends executing the thread of the Idle process in each sample interval, and subtracting that value from 100%. (Each processor has an Idle thread which consumes cycles when no other threads are ready to run.) It can be viewed as the percentage of the sample interval spent doing useful work. This counter displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time the service was inactive, and then subtracting that value from 100%.

Measurement	Description
File data Operations/sec	The rate that the computer issues Read and Write operations to file system devices. This does not include File Control Operations.
Interrupts/sec	The average number of hardware interrupts the processor receives and services per second. It does not include DPCs, which are counted separately. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended during interrupts. Most system clocks interrupt the processor every 10 milliseconds, creating a background of interrupt activity. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
Output Session Line Speed	This value represents the line speed from server to client for a session in bps.
Input Session Line Speed	This value represents the line speed from client to server for a session in bps.
Page Faults/sec	A count of the Page Faults in the processor. A page fault occurs when a process refers to a virtual memory page that is not in its Working Set in main memory. A Page Fault will not cause the page to be fetched from disk if that page is on the standby list, and hence already in main memory, or if it is in use by another process with whom the page is shared.

Measurement	Description
Pages/sec	The number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system Cache to access file data for applications. This value also includes the pages to/from non-cached mapped memory files. This is the primary counter to observe if you are concerned about excessive memory pressure (that is, thrashing), and the excessive paging that may result.
Pool Nonpaged Bytes	The number of bytes in the Nonpaged Pool, a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Nonpaged Pool pages cannot be paged out to the paging file, but instead remain in main memory as long as they are allocated.
Private Bytes	The current number of bytes this process has allocated that cannot be shared with other processes.
Processor Queue Length	The instantaneous length of the processor queue in units of threads. This counter is always 0 unless you are also monitoring a thread counter. All processors use a single queue in which threads wait for processor cycles. This length does not include the threads that are currently executing. A sustained processor queue length greater than two generally indicates processor congestion. This is an instantaneous count, not an average over the time interval.
Threads	The number of threads in the computer at the time of data collection. Notice that this is an instantaneous count, not an average over the time interval. A thread is the basic executable entity that can execute instructions in a processor.

Measurement	Description
Latency – Session Average	This value represents the average client latency over the life of a session.
Latency – Last Recorded	This value represents the last recorded latency measurement for this session.
Latency – Session Deviation	This value represents the difference between the minimum and maximum measured values for a session.
Input Session Bandwidth	This value represents the bandwidth from client to server traffic for a session in bps.
Input Session Compression	This value represents the compression ratio for client to server traffic for a session.
Output Session Bandwidth	This value represents the bandwidth from server to client traffic for a session in bps.
Output Session Compression	This value represents the compression ratio for server to client traffic for a session.
Output Session Linespeed	This value represents the line speed from server to client for a session in bps.

Virtual Channel Counters

The following table describes virtual channel counters:

Measurement	Description
Input Audio Bandwidth	This value represents the bandwidth from client to server traffic on the audio mapping channel. This is measured in bps.
Input Clipboard Bandwidth	This value represents the bandwidth from client to server traffic on the clipboard mapping channel. This is measured in bps.
Input COM1 Bandwidth	This value represents the bandwidth from client to server traffic on the COM1 channel. This is measured in bps.
Input COM2 Bandwidth	This value represents the bandwidth from client to server traffic on the COM2 channel. This is measured in bps.
Input COM Bandwidth	This value represents the bandwidth from client to server traffic on the COM channel. This is measured in bps.
Input Control Channel Bandwidth	This value represents the bandwidth from client to server traffic on the ICA control channel. This is measured in bps.
Input Drive Bandwidth	This value represents the bandwidth from client to server traffic on the client drive mapping channel. This is measured in bps.
Input Font Data Bandwidth	This value represents the bandwidth from client to server traffic on the local text echo font and keyboard layout channel. This is measured in bps.
Input Licensing Bandwidth	This value represents the bandwidth from server to client traffic on the licensing channel. This is measured in bps.
Input LPT1 Bandwidth	This value represents the bandwidth from client to server traffic on the LPT1 channel. This is measured in bps.

Measurement	Description
Input LPT2 Bandwidth	This value represents the bandwidth from client to server traffic on the LPT2 channel. This is measured in bps.
Input Management Bandwidth	This value represents the bandwidth from client to server traffic on the client management channel. This is measured in bps.
Input PN Bandwidth	This value represents the bandwidth from client to server traffic on the Program Neighborhood channel. This is measured in bps.
Input Printer Bandwidth	This value represents the bandwidth from client to server traffic on the printer spooler channel. This is measured in bps.
Input Seamless Bandwidth	This value represents the bandwidth from client to server traffic on the Seamless channel. This is measured in bps.
Input Text Echo Bandwidth	This value represents the bandwidth from client to server traffic on the local text echo data channel. This is measured in bps.
Input Thinwire Bandwidth	This value represents the bandwidth from client to server traffic on the Thinwire (graphics) channel. This is measured in bps.
Input VideoFrame Bandwidth	This value represents the bandwidth from client to server traffic on the VideoFrame channel. This is measured in bps.
Output Audio Bandwidth	This value represents the bandwidth from server to client traffic on the audio mapping channel. This is measured in bps.
Output Clipboard Bandwidth	This value represents the bandwidth from server to client traffic on he clipboard mapping channel. This is measured in bps.
Output COM1 Bandwidth	This value represents the bandwidth from server to client traffic on the COM1 channel. This is measured in bps.

Measurement	Description
Output COM2 Bandwidth	This value represents the bandwidth from server to client traffic on the COM2 channel. This is measured in bps.
Output COM Bandwidth	This value represents the bandwidth from server to client traffic on the COM channel. This is measured in bps.
Output Control Channel Bandwidth	This value represents the bandwidth from server to client traffic on the ICA control channel. This is measured in bps.
Output Drive Bandwidth	This value represents the bandwidth from server to client traffic on the client drive channel. This is measured in bps.
Output Font Data Bandwidth	This value represents the bandwidth from server to client traffic on the local text echo font and keyboard layout channel. This is measured in bps.
Output Licensing Bandwidth	This value represents the bandwidth from server to client traffic on the licensing channel. This is measured in bps.
Output LPT1 Bandwidth	This value represents the bandwidth from server to client traffic on the LPT1 channel. This is measured in bps.
Output LPT2 Bandwidth	This value represents the bandwidth from server to client traffic on the LPT2 channel. This is measured in bps.
Output Management Bandwidth	This value represents the bandwidth from server to client traffic on the client management channel. This is measured in bps.
Output PN Bandwidth	This value represents the bandwidth from server to client traffic on the Program Neighborhood channel. This is measured in bps.
Output Printer Bandwidth	This value represents the bandwidth from server to client traffic on the printer spooler channel. This is measured in bps.

Measurement	Description
Output Seamless Bandwidth	This value represents the bandwidth from server to client traffic on the Seamless channel. This is measured in bps.
Output Text Echo Bandwidth	This value represents the bandwidth from server to client traffic on the local text echo data channel. This is measured in bps.
Output Thinwire Bandwidth	This value represents the bandwidth from server to client traffic on the Thinwire (graphics) channel. This is measured in bps.
Output VideoFrame Bandwidth	This value represents the bandwidth from server to client traffic on the VideoFrame channel. This is measured in bps.

Part XIV

Middleware Performance Monitoring

41

Introduction to Middleware Performance Monitoring

Using LoadRunner's Middleware Performance monitors, you can monitor the Tuxedo and the IBM WebSphere MQ servers during a scenario run and isolate server performance bottlenecks.

A primary factor in a transaction's response time is the Middleware performance usage. LoadRunner's Middleware Performance monitors provide you with information about the Middleware performance usage of the Tuxedo and IBM WebSphere MQ servers during a scenario execution. To obtain performance data, you need to activate the online monitor for the server and specify which resources you want to measure before executing the scenario.

The Tuxedo monitor can monitor the server, load generator machine, workstation handler, and queue in a Tuxedo system. To run the Tuxedo monitor, you must install the Tuxedo client libraries on the machine you want to monitor.

The IBM WebSphere MQ monitor is used to monitor channel and queue performance counters on an IBM WebSphere MQ (version 5.x) Server.

The procedures for selecting monitor measurements and configuring the monitors vary according to server type. The following sections contain specific configuration instructions for each server type.

42

Tuxedo Monitoring

The Tuxedo monitor allows you to measure and view your Tuxedo server performance. It provides information about the host machine, workstation handler, and queue in a Tuxedo system.

To obtain data for this graph, you need to configure the Tuxedo monitor (from the Controller) and select the measurements you want to display, before running the scenario.

Note: If Tuxedo 7.1 or higher is installed on the Controller machine, more than one Tuxedo application server can be monitored at a time. However, if Tuxedo 6.5 or below is installed on the Controller machine, only one Tuxedo application server can be monitored at a time.

This chapter includes:

Setting up the Tuxedo Monitor

Before you set up the monitor, perform the following:

➤ Ensure that a Tuxedo workstation client (not a native client) is installed on the Controller machine. Use a Tuxedo 6.x client if a Tuxedo 6.x server is used, and Tuxedo 7.1 or above client if a Tuxedo 7.1 or above server is used. If you use a Tuxedo 6.5 or earlier server, you can still use a Tuxedo 7.1 or later client to monitor it, provided that you set the WSINTOPPRE71 environment variable to "yes".

Note: A Tuxedo workstation client communicates with the application server over the network, and is not required to run the Tuxedo application server on the same machine. A native client can only communicate with the Tuxedo application server if it is part of the relevant Tuxedo domain.

➤ Define the Tuxedo environment variables on the Controller machine—set the TUXDIR variable to the Tuxedo installation directory (for example, V:\environ\32\Tuxedo8.0), and add the Tuxedo **bin** directory to the PATH variable.

➤ Ensure that the workstation listener (WSL) process is running. This enables the application server to accept requests from workstation clients.

Note: The address and port number used to connect to the application server must match those dedicated to the WSL process.

Note: For information on configuring the WSL, refer to the BEA Tuxedo Web site (http://edocs.beasys.com/tuxedo/tux81/rf5/rf5101.htm#1534543).

Adding a Machine to Monitor

In order to monitor the Tuxedo resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the Tuxedo graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The Tuxedo dialog box opens.
3. In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
4. Enter the server name or IP address of the machine you want to monitor.

Note: If you are using multiple instances of the Tuxedo monitor on the same machine, then enter the port number of each Tuxedo monitor in order to distinguish one instance from another. The entry should have the following format: <machine name>:<port number>

Select the platform on which the machine runs, and click **OK**.

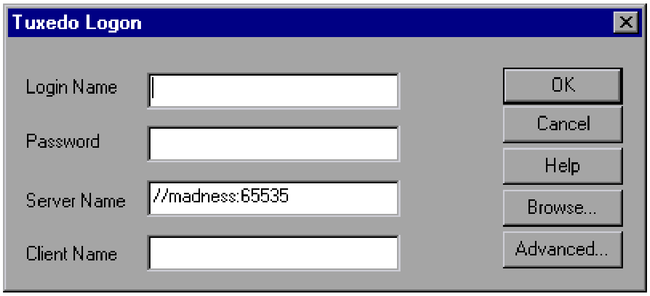
5. In the **Resource Measurements** section of the Tuxedo dialog box, click **Add**.
6. Continue with "Configuring the Tuxedo Monitor" on page 362.

Configuring the Tuxedo Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the Tuxedo monitor:

1 When you click **Add** to add a measurement, the Tuxedo Logon dialog box opens.



Enter the following information:

➤ **Login Name:** Enter your login name.

➤ **Password:** Enter your password.

➤ **Server Name:** Enter the name of the server. The format of the server name is //<machine name>:<port number>. Alternatively, you can specify the IP address or the hexadecimal format used by old versions of Tuxedo.

Note: You cannot use quotation marks.

➤ **Client Name:** Enter the name of the client machine. If a Tuxedo server was previously monitored, its name is displayed in the Server Name box.

➤ **Browse**: Enables you to navigate to the tpinit.ini file of a recorded Tuxedo script.

Note: Logon information is located in the Logon section of the **tpinit.ini** file in the recorded script's directory. It is recommended that you use the Browse button and select the **tpinit.ini** file from a recorded script, rather than enter the values manually. You can also determine the client name from the **lrt_tpinitialize** statement in the recorded script.

In the following example of a **tpinit.ini** file, the Tuxedo monitor was configured for a server named psft1 using port 7000, and a client named bankapp. The logon user name was PS and the password was PS.

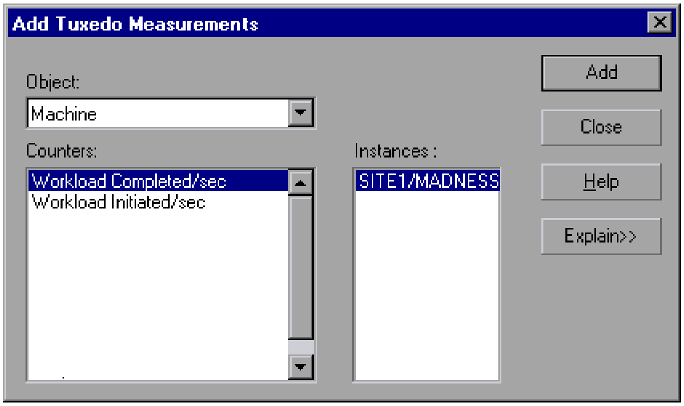
```
[Logon]
LogonServername=//psft1:7000
LogonUsrName=PS
LogonCltName=bankapp
LogonGrpName=
LogonPasswd=PS
LogonData=
```

2 To authenticate the Tuxedo monitor, click **Advanced**, and enter the authentication data as a hexadecimal string (beginning with "0x") in the data box. The authentication data value can be obtained from the **tpinit.ini** file of an existing Tuxedo script.

Note: If you are using Tuxedo 6.5 or below, the monitor can only connect to one application server during a scenario. Once it connects to an application server, the server is the only one used by the monitor until the Controller is closed. This applies even when all of the counters are deleted from the monitor.

---

3 Click **OK**. The Add Tuxedo Measurements dialog box opens.



4 For each measurement, select an object, counter, and instance, and then click **Add**, as described in "Understanding the Add Tuxedo Measurements Dialog Box" on page 364.

For a description of the available measurements, see "Tuxedo Performance Counters" on page 365.

5 Add all the desired objects to the list, and click **Close**. The measurements that you selected appear in the **Resource Measurements on**: <*machine*> section of the Tuxedo dialog box.

6 Click **OK** in the Tuxedo dialog box to activate the monitor.

Understanding the Add Tuxedo Measurements Dialog Box

The Add Tuxedo Measurements dialog box lets you select the resources to monitor on the Tuxedo client.

- **Object.** Select the object being monitored on the specified machine.
- **Counters.** Select a resource counter to monitor. Select multiple counters using the CTRL key. For an explanation of each counter, click **Explain**.
- **Instances.** If multiple instances of the selected counter are running, select one or more instances to monitor for the selected counter.
- **Explain.** Displays a description of the selected counter.

Tuxedo Performance Counters

The following table lists the available Tuxedo monitor measurements. It is recommended to pay particular attention to the following measurements: % Busy Clients, Active Clients, Busy Clients, Idle Clients, and all the queue counters for relevant queues:

Monitor	Measurements
Machine	**% Busy Clients** - The percent of active clients currently logged in to the Tuxedo application server that are waiting for a response from the application server.
	Active Clients - The total number of active clients currently logged in to the Tuxedo application server.
	Busy Clients - The total number of active clients currently logged in to the Tuxedo application server that are waiting for a response from the application server.
	Current Accessers - The number of clients and servers currently accessing the application either directly on this machine or through a workstation handler on this machine.
	Current Transactions - The number of in-use transaction table entries on this machine.
	Idle Clients - The total number of active clients currently logged in to the Tuxedo application server that are not waiting for a response from the application server.
	Workload Completed/second - The total workload on all the servers for the machine that was completed, per unit time.
	Workload Initiated/second - The total workload on all the servers for the machine that was initiated, per unit time.

Monitor	Measurements
Queue	**% Busy Servers** - The percent of active servers currently handling Tuxedo requests.
	Active Servers - The total number of active servers either handling or waiting to handle Tuxedo requests.
	Busy Servers - The total number of active servers currently busy handling Tuxedo requests.
	Idle Servers - The total number of active servers currently waiting to handle Tuxedo requests.
	Number Queued - The total number of messages which have been placed on the queue.
Server	**Requests/second** -The number of server requests handled per second
	Workload/second - Workload is a weighted measure of the server requests. Some requests could have a different weight than others. By default, the workload is always 50 times the number of requests.
Workstation Handler (WSH)	**Bytes Received/sec** - The total number of bytes received by the workstation handler, per second.
	Bytes Sent/sec - The total number of bytes sent back to the clients by the workstation handler, per second.
	Messages Received/sec - The number of messages received by the workstation handler, per second.
	Messages Sent/sec - The number of messages sent back to the clients by the workstation handler, per second.
	Number of Queue Blocks/sec - The number of times the queue for the workstation handler blocked, per second. This gives an idea of how often the workstation handler was overloaded.

43

IBM WebSphere MQ Monitoring

The IBM WebSphere MQ monitor displays statistics about the resource usage on the IBM WebSphere MQ server during the scenario run.

To use the IBM WebSphere MQ monitor you must first install the IBM WebSphere MQ client on the Controller machine and configure the server environment to monitor events. The IBM WebSphere MQ monitor connects to the IBM WebSphere MQ server (via the MQ Client Connection installed on the Controller machine). In MQ Client environments, the client machine connects to an MQ Server instance, and uses the Server's resources as if they were local to the client machine.

You can then enable the MQ online monitor (from the Controller) and select the measurements you want to display, before running the scenario.

Note: The LoadRunner IBM WebSphere MQ monitor supports machines running the IBM MQ Server (version 5.2) on Windows platforms only.
To monitor the IBM WebSphere MQ server, the Windows user must be part of the Administration Group of the IBM WebSphere MQ server.

This chapter includes:

Setting up the Monitoring Environment

Before you set up the monitor, perform the following:

➤ Ensure that an IBM WebSphere MQ Client Connection (version 5.21 only) is installed on the Controller machine.

For additional information on installing the IBM WebSphere MQ Server/Client, refer to the IBM Web site (http://www.ibm.com/).

➤ Configure the IBM WebSphere server to monitor events.

The LoadRunner MQ Monitor retrieves event messages from two standard MQSeries queues only:

➤ SYSTEM.ADMIN.PERFM.EVENT – performance events, such as “queue depth high”

➤ SYSTEM.ADMIN.CHANNEL.EVENT – channel events, such as “channel stopped”

Events must be enabled for the queue manager (and in many cases, on the applicable object, as well). Performance events are enabled by setting attributes for the queue on the MQ Server. Channel events are enabled by default, and cannot be disabled.

Note: The IBM WebSphere MQ monitor does not retrieve data from a queue manager after the queue manager has been restarted.

To enable performance events for the Queue Manager:

1. Use the following MQSC command: ALTER QMGR PERFMEV(ENABLED).
2. Set the following attributes for the queue:

Measurement	Set Event Attributes
Event - Queue Depth High	➤ QDEPTHHI(integer) – where integer is a value expressed as a percentage of maximum messages allowed, and is in the range of 0 to 100 inclusive. ➤ QDPHIEV(action) – where action is the word “ENABLED” or “DISABLED”, enabling or disabling the generation of the event, respectively.
Event - Queue Depth Low	To enable the event for a queue, the following attributes of the queue must be set: ➤ QDEPTHLO(integer) – where integer is a value expressed as a percentage of maximum messages allowed, and is in the range of 0 to 100 inclusive. ➤ QDPLOEV(action) – where action is the word “ENABLED” or “DISABLED”, enabling or disabling the generation of the event, respectively.
Event - Queue Full	➤ QDEPTHHI(integer) – where integer is a value expressed as a percentage of maximum messages allowed, and is in the range of 0 to 100 inclusive. ➤ QDPMAXEV(action) – where action is the word “ENABLED” or “DISABLED”, enabling or disabling the generation of the event, respectively.

Measurement	Set Event Attributes
Event - Queue Service Interval High	➤ QSVCINT(integer) – where integer is a value expressed as milliseconds, in the range of 0 and 999,999,999, inclusive. Note: this value is shared with Queue Service Interval OK. ➤ QSVCIEV(type) – where type is the word "HIGH", "OK", or "NONE", enabling service interval high events, enabling service interval ok events, or disabling the generation of the event, respectively.
Event - Queue Service Interval OK	➤ QSVCINT(integer) – where integer is a value expressed as milliseconds, in the range of 0 and 999,999,999, inclusive. Note: this value is shared with Queue Service Interval High. ➤ QSVCIEV(type) – where type is the word "HIGH", "OK", or "NONE", enabling service interval high events, enabling service interval ok events, or disabling the generation of the event, respectively.

Note: If you encounter an MQ Server error message (starting with the characters MQRC_), refer to the WebSphere MQ family support Web site (http://www-306.ibm.com/software/integration/mqfamily/support/).

After you have installed the MQ Client on the Controller, and configured the server environment to monitor events, you can specify which resources you want to measure.

Adding a Machine to Monitor

In order to monitor the IBM WebSphere MQ resources of a particular machine from the Controller, you need to add the machine and the measurements that you want to monitor.

To add a machine to the Controller:

1. Click the IBM WebSphere MQ graph in the graph tree, and drag it into the right pane of the Run view.
2. Right-click the graph and select **Add Measurements**, or click anywhere on the graph and choose **Monitors** > **Add Measurements**. The IBM WebSphere MQ dialog box opens.

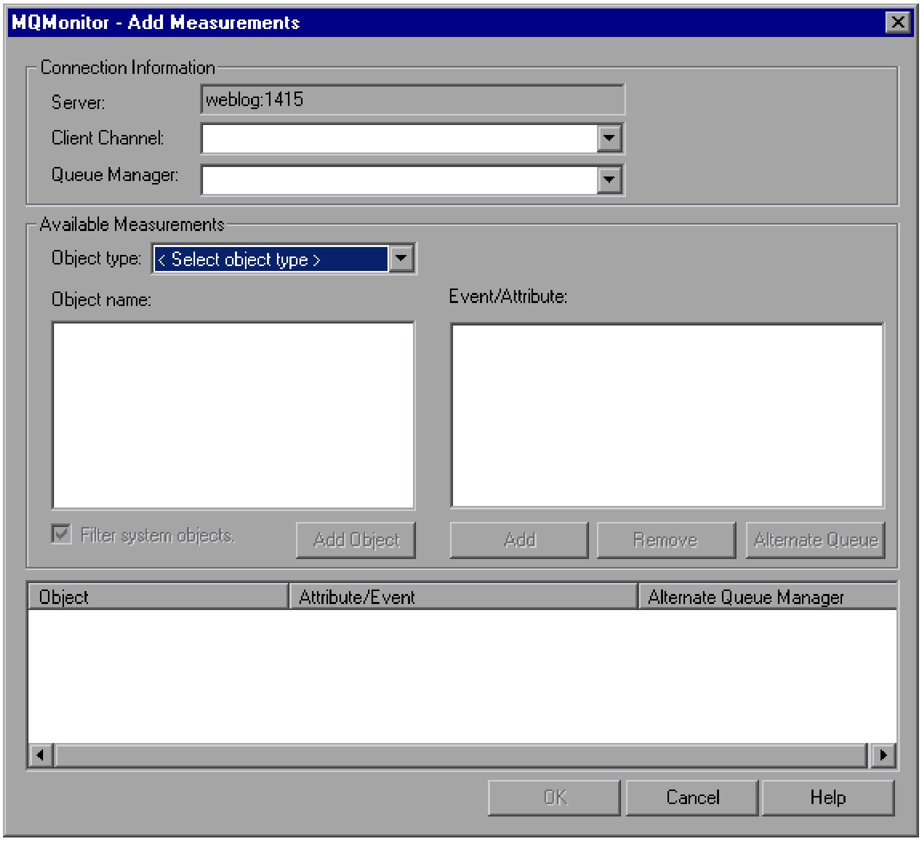
   In the **Monitored Server Machines** section, click **Add.** The Add Machine dialog box opens.
3. Enter the server name or IP address of the machine you want to monitor. The format of the server name is <machine name>:<port number>. Select the platform on which the machine runs, and click **OK**.
4. In the Resource Measurements section of the IBM WebSphere MQ dialog box, click **Add**.
5. Continue with "Configuring the IBM WebSphere MQ Monitor" on page 372.

Configuring the IBM WebSphere MQ Monitor

After you have added the machine that you are monitoring, you configure the monitor by choosing which measurements to monitor on the machine.

To configure the IBM WebSphere MQ monitor:

1 When you click **Add** to add a measurement, the MQMonitor - Add Measurements dialog box opens.



In the **Connections Information** section, enter the name of the channel through which a client connection is made to an MQ Server, and the name of the queue manager to be monitored.

Note: A queue manager can only be accessed by one Controller or monitoring application at any one time.

User entries for any text box are limited to 48 characters.

---

2 In the **Available Measurements** section, select an object type.

A list of previously added objects of the selected object type appear in the **Object name** list. A list of attributes or events applicable to the selected object type appear in the **Events/Attributes** list.

The names of monitored objects, event/attribute selected, and alternate queue managers, are listed in the monitored objects pane.

3 By default, only user-defined objects are displayed in the Object name list. To show all objects, clear the **Filter System Objects** check box. You can modify the filter settings, in the **<LoadRunner_installation>\dat\monitors\mqseries.cfg** file.

4 Select an object or add a new object to the Object name list. To add a new object name, click **Add Object**. In the Add Object Name dialog box, enter the name of an object to be monitored and click **OK**. The dialog box closes and the name of the object appears in the **Object name** list.

5 Select the attributes or events to be measured from the **Attribute/Event** box. The list of attributes or events is applicable to the selected object type.

For a description of the available measurements, see "IBM WebSphere MQ Performance Counters" on page 376.

Note: To enable the event for a queue, ensure that the attributes for the queue have been set. For more information, refer to "Setting up the Monitoring Environment" on page 368.

---

6 If the event configured for monitoring is from a remote queue manager (other than the one identified in the queue manager field of the IBM WebSphere MQ Add Measurements dialog box), click **Alternate Queue**. Enter the name of an alternate queue manager in the Alternate Queue dialog box, and click **OK**.

Note: When you add an alternate queue manager, this becomes the default queue manager for any events that you subsequently add. To return to the queue manager to which you are connected, enter that name in the Alternate Queue Manager dialog box.

---

7 To add the object measurements to the monitored objects list, click **Add**. The name of the object, it's events and attributes, and any alternate queue managers, are listed in the monitored objects pane.

8 To remove a monitored object event or attribute, select the object measurement in the monitored objects pane, and click **Remove**. The entry is deleted from the monitored objects list.

9 Add all the desired counters to the monitored objects list, and click **OK**. The measurements that you selected appear in the **Resource Measurements on**: *<machine>* section of the IBS WebSphere MQ dialog box.

10 Click **OK** in the IBM WebSphere MQ dialog box to activate the monitor.

Understanding the MQMonitor - Add Measurements Dialog Box

The MQMonitor - Add Measurements dialog box lets you select the items to monitor on the IBM WebSphere MQ server.

Connection Information

- **Server.** The name of the server you are monitoring.
- **Client Channel.** Enter the name of the channel through which a client connection is made to an MQ Server.

Note: You can set up a specific channel on an MQ Server instance, or use the default "SYSTEM.DEF.SVRCONN" channel. If the client channel is undefined, the MQ Server will be inaccessible via client connections (the MQ Monitor will not work, as it will not be able to connect to the queue manager which it is supposed to monitor).

- **Queue Manager.** Enter the name of the queue manager to be monitored.

Note: The monitor is not restricted to monitoring only the queue manager to which it is connected. You can configure multiple queue managers to write to the event queue of a central queue manager for centralized monitoring (this applies to Events only, not polled object attributes). All events contain a queue manager attribute identifying their source.

Available Measurements

- **Object Type.** Select an object type from either Channel or Queue.
- **Object Name.** Enter a name for object you want to monitor.
- **Event/Attribute.** Select the events and attributes you want to monitor.
- **Filter System Objects.** Select to enable the system objects filter.
- **Add Object.** Enables you to add a new object name to the Object name list.

- **Add.** Enables you to add an Event or Attribute to an object.
- **Remove.** Enables you to remove a monitored object event or attribute from the Object name list.
- **Alternate Queue.** Enter the name of an alternate queue manager if the event is from a remote queue manager.

Monitored Object list

A list of monitored objects, including the object's name, events and attributes, and alternate queue manager.

IBM WebSphere MQ Performance Counters

The following tables list the available IBM WebSphere MQ monitor measurements:

Queue Performance Counters

The following table describes the Queue Performance counters:

Measurement	Description
Event - Queue Depth High (events per second)	An event triggered when the queue depth reaches the configured maximum depth.
Event - Queue Depth Low (events per second)	An event triggered when the queue depth reaches the configured minimum depth.
Event - Queue Full (events per second)	An event triggered when an attempt is made to put a message on a queue that is full.
Event - Queue Service Interval High (events per second)	An event triggered when no messages are put to or retrieved from a queue within the timeout threshold.
Event - Queue Service Interval OK (events per second)	An event triggered when a message has been put to or retrieved from a queue within the timeout threshold.

Measurement	Description
Status - Current Depth	Current count of messages on a local queue. This measurement applies only to local queues of the monitored queue manager.
Status - Open Input Count	Current count of open input handles. Input handles are opened so that an application may "put" messages to a queue.
Status - Open Output Count	Current count of open output handles. Output handles are opened so that an application may "get" messages from a queue.

Channel Performance Counters

The following table describes the Channel Performance counters:

Measurement	Description
Event - Channel Activated (events per second)	Event generated when a channel, waiting to become active but inhibited from doing so due to a shortage of queue manager channel slots, becomes active due to the sudden availability of a channel slot.
Event - Channel Not Activated (events per second)	Event generated when a channel, attempts to become active but inhibited from doing so due to a shortage of queue manager channel slots.
Event - Channel Started (events per second)	Event generated when a channel is started.
Event - Channel Stopped (events per second)	Event generated when a channel is stopped, regardless of source of stoppage.
Event - Channel Stopped by User (events per second)	Event generated when a channel is stopped by a user.
Status - Channel State	The current state of a channel. Channels pass through several states from STOPPED (inactive state) to RUNNING (fully active state). Channel states range from 0 (STOPPED) to 6 (RUNNING).

Measurement	Description
Status - Messages Transferred	The count of messages that have been sent over the channel. If no traffic is occurring over the channel, this measurement will be zero. If the channel has not been started since the queue manager was started, no measurement will be available.
Status - Buffer Received	The count of buffers that have been received over the channel. If no traffic is occurring over the channel, this measurement will be zero. If the channel has not been started since the queue manager was started, no measurement will be available.
Status - Buffer Sent	The count of buffers that have been sent over the channel. If no traffic is occurring over the channel, this measurement will be zero. If the channel has not been started since the queue manager was started, no measurement will be available.
Status - Bytes Received	The count of bytes that have been received over the channel. If no traffic is occurring over the channel, this measurement will appear as zero. If the channel has not been started since the queue manager was started, no measurement will be available.
Status - Bytes Sent	The count of bytes that have been sent over the channel. If no traffic is occurring over the channel, this measurement will appear as zero. If the channel has not been started since the queue manager was started, no measurement will be available.

Part XV

Infrastructure Resource Monitoring

44

Infrastructure Resources Monitoring

Using LoadRunner's Network Client monitor, you can monitor network client resources for FTP, POP3, SMTP, IMAP, and DNS Vusers during a scenario run and isolate client performance bottlenecks.

This chapter includes:

Configuring the Network Client Monitor

The Network Client online monitor graph is only available during scenarios that run relevant scripts, such as FTP, POP3, and so forth.

You can view this graph by dragging it from the Infrastructure Resources Graph section in the graph tree into the right pane of the Run view. The graph appears in the graph view area.

Network Client Performance Counters

The following table describes the Network Client measurements that are monitored:

Measurement	Description
Pings per sec	Number of pings per second
Data transfer bytes per sec	Number of data bytes transferred per second

Measurement	Description
Data receive bytes per sec	Number of data bytes received per second
Connections per sec	Number of connections per second
Accept connections per sec	Number of connections accepted per seconds
SSL Connections per sec	Number of SSL connections per second
SSL Data transfer bytes per sec	Number of SSL data bytes transferred per second
SSL Data receive bytes per sec	Number of SSL data bytes received per second
SSL Accept connections per sec	Number of SSL connections accepted per seconds

Part XVI

Appendixes

A

Troubleshooting Online Monitors

LoadRunner monitors allow you to view the performance of the scenario during execution.

The following sections describe several tips and known issues relating to the online monitors.

This appendix includes:

Troubleshooting Server Resource Monitors

To monitor resources on a server machine, you must be able to connect to that machine. If monitoring is unsuccessful and LoadRunner cannot locate the specified server, make sure that the specified server is available. Perform a "ping" operation by typing ping <server_name> from the Controller machine command line.

Once you verify that the machine is accessible, check this table for additional tips on troubleshooting the monitor.

Problem	Solution
Cannot monitor a Windows machine on a different domain, or "access denied."	To gain administrative privileges to the remote machine, perform the following from the command prompt: %net use \\<MachineName>/ user:[<Domain>\<RemoteMachineUsername>] At the password prompt, enter the password for the remote machine.
Cannot monitor a Windows machine (An error message is issued: "computer_name not found" or "Cannot connect to the host")	The Windows machine you want to monitor only enables monitoring for users with administrator privileges. To allow monitoring for non-admin users, you must grant read permission to certain files and registry entries (Microsoft tech-note number Q158438.) The required steps are: **a.** Using Explorer or File Manager, give the user READ access to: %windir%\system32\PERFCxxx.DAT %windir%\system32\PERFHxxx.DAT where xxx is the basic language ID for the system—for example, 009 for English. These files may be missing or corrupt. If you suspect this; expand these files off of the installation cd. **b.** Using REGEDT32, give the user READ access to: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib and all sub keys of that key. **c.** Using REGEDT32, give the user at least READ access to: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg

Problem	Solution
Some Windows default counters are generating errors	Remove the problematic counters and add the appropriate ones using the "Add Measurement" dialog box.
You cannot get performance counters for the SQL server (version 6.5) on the monitored machine.	There is a bug in SQL server version 6.5. As a workaround, give read permission to the following registry key at the monitored machine (use regedt32): HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer (Microsoft tech-note number Q170394)
The selected measurements are not displayed in the graph.	Ensure that the display file and online.exe are registered. To register the monitor dll's, without performing a full installation, run the **set_mon.bat** batch file located in **LoadRunner\bin**.
When monitoring a Windows machine, no measurements appear in the graph.	Check the built-in Windows Performance Monitor. If it is not functional, there may be a problem with the communication setup.
When monitoring a UNIX machine, no measurements appear in the graph.	Ensure that an **rstatd** is running on the UNIX machine (Refer to Part IV, "System Resource Monitoring.")
Cannot monitor one of the following Web servers: MS IIS, MS ASP, or ColdFusion	Refer to problem above, "Cannot monitor a Windows machine."

Problem	**Solution**
Cannot monitor the WebLogic (JMX) server	Open the **<LoadRunner root folder>\dat\monitors\WebLogicMon.ini** file, and search for: [WebLogicMonitor] JVM=javaw.exe Change javaw.exe to java.exe. A window containing trace information opens.

Troubleshooting the Network Delay Monitor

If monitoring is unsuccessful and LoadRunner cannot locate the source or destination machines, make sure that the specified machines are available to your machine. Perform a "ping" operation. At the command line prompt, type:

```
ping server_name
```

To check the entire network path, use the trace route utility to verify that the path is valid.

For Windows, type tracert <server_name>.

For UNIX, type traceroute <server_name>.

If the monitoring problem persists once you verify that the machines are accessible and that the network path is valid, perform the following procedures:

1. If you are using the TCP protocol, run <**LoadRunner root folder**>**\bin\webtrace.exe** from the source machine to determine whether the problem is related to the Controller, or the WebTrace technology on which the Network Delay monitor is based. If you are using the UDP or ICMP protocols, the problem must be related to the Controller and not WebTrace, since these protocols are not WebTrace technology-based.

2. If you receive results by running **webtrace.exe**, the problem is related to the Controller. Verify that the source machine is not a UNIX machine, and contact the Customer Support Web site with the following information:

   ➤ the Controller log file, **drv_log.txt**, located in the **temp** directory of the Controller machine.

   ➤ the **traceroute_server** log file, located on the source machine.

   ➤ the debug information located in the **TRS_debug.txt** and **WT_debug.txt** files in the path directory. These files are generated by adding the following line to the [monitors_server] section of the <**LoadRunner root**

folder>\dat\mdrv.dat file, and rerunning the Network monitor:

ExtCmdLine=-traceroute_debug path

3 If you do not receive results by running **webtrace.exe**, the problem is related to the WebTrace technology, on which the Network Delay monitor is based. Perform the following procedures on the source machine:

- Verify that the **packet.sys** file (the Webtrace driver) exists in the **WINNT\system32\drivers** directory.
- Check whether a driver (such as “Cloud” or “Sniffer”) is installed on top of the network card driver. If so, remove it and run WebTrace again.
- Verify that there are administrator permissions on the machine.
- Using ipconfig /all, check that only one IP address is assigned to the network card. WebTrace does not know how to handle multiple IP addresses assigned to the same card (IP spoofing).
- Check the number of network cards installed. Run webtrace –devlist to receive a list of the available network cards.
- If there is more than one card on the list, run webtrace -dev <dev_name> <destination>, where <dev_name> is one of the network card names shown in the list. If you discover that WebTrace is binding to the wrong card, you can use webtrace set_device <dev_name> to set a registry key that instructs WebTrace to use a specified card instead of the default one.
- Verify that the network card is of the Ethernet type.
- Contact the Customer Support Web site with the output of webtrace.exe –debug (for example, webtrace.exe –debug www.merc-int.com) and ipconfig /all on the machine.

Network Considerations

If you notice extraordinary delays on the network, refer to one of the following sections to increase the performance:

- Network Bandwidth Utilization
- Ethernet-bus Based Networks

➤ Working on a WAN or Heavily Loaded LAN

Network Bandwidth Utilization

In most load-testing scenario, the network card has little impact on scenario performance. Network cards are manufactured to handle the bandwidth of the physical network layer. Packets are transferred over an Ethernet at a rate that complies with IEEE 803.x standards. If the network becomes a bottleneck, the issue is not the brand of the network card, but rather the bandwidth limitations on the physical layer (--i.e. Ethernet, FDDI, ATM, Ethernet Token-ring, etc.).

That is, instead of load testing over a T10 line, upgrade your line to DS3 (45Mbps), or T100 (100Mbps).

Below are a few tips that will help qualify the need to upgrade the network:

1 Run the performance monitor on the Vuser load generators. As the number of Vusers increases, check the network byte transfer rate for saturation. If a saturation point has been reached, do not run any more Vusers without upgrading the network—otherwise performance of Vusers will degrade. Degradation is exponential in networking environments.

2 Run the performance monitor on the server machine. Run many Vusers on several load generator machines. Check the kernel usage and network transfer rate for saturation. If saturation is reached with less than the desired Vuser load, upgrade the network.

3 Every network has a different Maximum Transmission Unit or MTU, which is set by the network administrator. The MTU is the largest physical packet size (in bytes) that a network can transmit. If a message is larger than the MTU, it is divided into smaller packets before being sent.

If clients and servers are passing large data sets back and forth, instruct the network administrator to increase the MTU to yield better bandwidth utilization. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination.

If you send a message that is larger than one of the MTUs, it will be broken up into fragments, slowing transmission speeds. If the MTU is too high, it may cause unintended degradation. Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, most Ethernet networks have an MTU of 1500.

If the desired MTU reduces performance, upgrade the network or reduce the MTU to improve performance.

Ethernet-bus Based Networks

The following guidelines apply to Ethernet-bus based networks:

Networks with only 2 active machines communicating yield a maximum of 90% bandwidth utilization.

Networks with 3 active machines communicating yield a maximum of approximately 85% bandwidth utilization.

As the number of active machines on the network increases, the total bandwidth utilization decreases.

Working on a WAN or Heavily Loaded LAN

When you work with LoadRunner on a WAN or heavy loaded LAN, you may notice some unusual LoadRunner behavior, which indicates network problems. The Output window may contain messages about retries, lost packets, or message mismatch. This is because some of the messages from the Controller may not be reaching the LoadRunner agent. To solve this problem, you should reduce the network traffic or improve the network bandwidth.

The following steps may help reduce network traffic:

- Click the **Run-Time Settings** button and select the **General: Log** node. Clear the **Enable logging** check box.
- Initialize all users before running them. Run them only after initialization is completed.

B

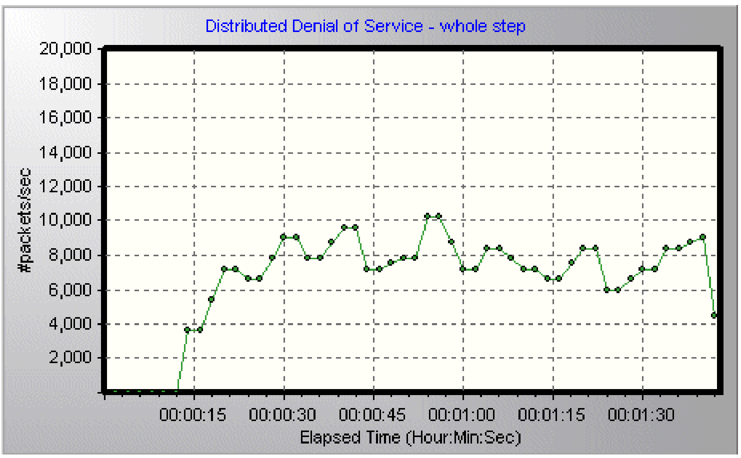
Security Monitoring

When you run certain security scripts, you can use LoadRunner's security graphs to view information about the simulated attacks on the server.

Distributed Denial of Service Graph

The Distributed Denial of Service graph displays the number of packets per second sent to the specified target to cause denial of service.

The x-axis represents the elapsed time. The y-axis represents the number of packets sent per second.



Note: To obtain data for this graph, you need to execute one of the following canned security scripts: SYN FLOOD DDOS Attack or UDP Echo DDOS Attack.

C

Working with Server Monitor Counters

When you configure the System Resource, Microsoft IIS, Microsoft ASP, ColdFusion, and SQL Server monitors, you are presented with a list of default counters that you can measure on the server you are monitoring. Using the procedure described below, you can create a new list of default counters by including additional counters, or deleting existing counters.

In addition, there are specific counters that are especially useful for determining server performance and isolating the cause of a bottleneck during an initial stress test on a server.

This appendix includes:

Changing a Monitor's Default Counters

You can change the default counters for the System Resource, Microsoft IIS, Microsoft ASP, or SQL Server monitors by editing the **res_mon.dft** file found in the **LoadRunner\dat** directory.

To change the default counters:

1. Open a new scenario and click the **Run** tab.
2. For each of the monitors, select the counters you want to measure.
3. Save the scenario and open the scenario **.lrs** file with an editor.

4 Copy the MonItemPlus section of the each counter you selected into the **res_mon.dft** file.

5 Count the number of new counters in the file and update the **ListCount** parameter with this number.

Useful Counters for Stress Testing

Certain counters are especially useful for determining server performance and isolating the cause of a bottleneck during an initial stress test on a server.

The following is a list of counters that are useful for monitoring Web server performance:

Object	Counter
Web Service	Maximum Connections
Web Service	Bytes Total/sec
Web Service	Current NonAnonymous Users
Web Service	Current Connections
Web Service	Not Found Errors
Active Server Pages	Requests/sec
Active Server Pages	Errors/sec
Active Server Pages	Requests Rejected
Active Server Pages	Request Not Found
Active Server Pages	Memory Allocated
Active Server Pages	Requests Queued
Active Server Pages	Errors During Script Run Time
Memory	Page Faults/sec
Server	Total Bytes/sec
Process	Private Bytes/Inetinfo

The following is a list of counters that are useful for monitoring SQL Server performance:

Object	Counter
SQLServer	User Connections
SQLServer	Cache Hit Ratio
SQLServer	Net-Network Reads/sec
SQLServer	I/O-Lazy Writes/sec
SQLServer-Locks	Total Blocking Locks
PhysicalDisk	Disk Queue Length

The following is a list of counters that are useful for monitoring both Web and SQL server performance:

Object	Counter
Processor	% Total Processor Time
PhysicalDisk	% Disk Time
Memory	Available Bytes
Memory	Pool Nonpaged Bytes
Memory	Pages/sec
Memory	Committed Bytes
System	Total Interrupts/sec
Object	Threads
Process	Private Bytes:_Total

Note: The % Disk Time counter requires that you run the diskperf -y utility at the command prompt and reboot your machine.

Index

U

V

W