

Internet Express

Internet Monitor Administrator's Guide

December 2003

Product Version: Internet Monitor Version 1.7

Operating System and Version: HP Tru64 UNIX Version 5.1A and higher

This document describes how to install, configure, and use the Internet Monitor software.

© Copyright 2003 Hewlett-Packard Development Company, L.P.

Microsoft® and Windows NT® are trademarks of Microsoft Corporation in the U.S. and/or other countries. Intel®, Pentium®, and Intel Inside® are trademarks of Intel Corporation in the U.S. and/or other countries. UNIX® and The Open Group™ are trademarks of The Open Group in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective owners.

Proprietary computer software. Valid license from HP and/or its subsidiaries 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.

Neither HP nor any of its subsidiaries shall be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Contents

About This Manual

1 Introduction to the Internet Monitor

1.1	Data Collection Agents	1-2
1.2	Data Collection Server	1-4
1.3	Performance Monitor	1-4
1.4	Historical Report Generation Tools	1-6
1.5	Getting Started with the Internet Monitor	1-9

2 Installing the Internet Monitor

2.1	Prerequisites	2-1
2.2	Choosing an Installation Interface	2-1
2.3	Installing the Internet Monitor	2-1
2.4	Installing Agent Software	2-2
2.5	Installing the Performance Monitor Application	2-3
2.6	Configuring the Agent to Restart Automatically on a UNIX System .	2-4

3 Deployment Guidelines

3.1	Sampler Database Sizing Guidelines	3-1
3.2	Data Collection Agent Deployment Guidelines	3-1
3.2.1	Determining the Location for Installation of the Data Collection Agent	3-1
3.2.2	Determining the Number of Agents to Deploy	3-2
3.2.3	Autostarting Agents After Installation	3-2
3.3	Sampler Configuration Guidelines	3-2
3.3.1	Determining a Sampling Interval	3-3
3.3.2	Determining the Data to be Retrieved by a Sampler	3-3
3.3.3	HTTP Sampler Deployment Guidelines	3-3
3.3.4	NNTP Sampler Deployment Guidelines	3-3
3.3.4.1	Creating a Newsgroup	3-3
3.3.4.2	Limiting Export of a Newsgroup	3-4
3.3.4.3	Modifying Article Expiration Definitions for the Target Newsgroup	3-4
3.3.4.4	Posting Sample Messages to the Target Newsgroup	3-4
3.3.5	POP and IMAP Sampler Deployment Guidelines	3-4
3.3.6	Creating Target User Accounts for SMTP, POP, and IMAP Samplers	3-4
3.3.6.1	Creating a UNIX Target User Account	3-5
3.3.6.2	Configuring E-Mail for the Target User Account	3-5
3.3.6.3	Populating a Target User Account with Test Messages	3-5
3.3.6.4	Disposing of Any New SMTP Messages	3-5
3.3.6.4.1	Using the slocal Command to Filter Incoming E-Mail	3-6
3.3.6.4.2	Using the procmail Command to Filter Incoming E-Mail	3-6
3.3.6.5	Improving Security for Target User Accounts	3-7
3.3.7	SMTP Sampler Deployment Guidelines	3-7
3.3.8	FTP Sampler Deployment Guidelines	3-7

3.3.9	RADIUS Sampler Deployment Guidelines	3-7
3.3.10	Connection Sampler Deployment Guidelines	3-8
3.4	Threshold Configuration Guidelines	3-8
3.5	Security Guidelines	3-9
3.6	Configuring the Internet Monitor for Use in a Firewalled Environment	3-9
3.7	Configuring the Internet Monitor to Use Alternate Databases	3-11
3.7.1	Install and Configure the Database Product	3-11
3.7.2	Create the Samples and Configuration Databases	3-11
3.7.3	Configure the Samples and Configuration Databases	3-11
3.7.4	Prepare the Internet Monitor	3-12
3.7.5	Install the Appropriate JDBC Driver	3-13
3.7.6	Modify the Internet Monitor Properties File	3-13
3.7.7	Start the Internet Monitor and Verify Proper Functionality	3-15
3.7.8	Implement Samples Database Archiving	3-16
3.8	Using the Java Message Service	3-16
3.8.1	Contents of the SampleReceived Message	3-16
3.8.2	Properties of the SampleReceived Message Body	3-17
3.8.3	Contents of the ThresholdChanged Message	3-18
3.8.4	Properties of the ThresholdChanged Message Body	3-18
3.8.5	Accessing the JMS Class Files	3-20
3.8.6	Running the Sample JMS Client Application	3-20
3.8.7	Specifying the JMS Configuration	3-20
3.9	Using the Performance Monitor Applet in a Cluster Environment ..	3-21

4 Administering the Internet Monitor

4.1	Starting and Stopping the Internet Monitor	4-1
4.2	Accessing the Internet Monitor	4-1
4.3	Defining Sampling Parameters	4-2
4.3.1	Managing HTTP Samplers	4-3
4.3.1.1	Creating an HTTP Sampler	4-4
4.3.1.2	Modifying or Removing an HTTP Sampler	4-6
4.3.2	Managing NNTP Samplers	4-6
4.3.2.1	Creating an NNTP Sampler	4-7
4.3.2.2	Modifying or Removing an NNTP Sampler	4-8
4.3.3	Managing POP Samplers	4-8
4.3.3.1	Creating a POP Sampler	4-9
4.3.3.2	Modifying or Removing a POP Sampler	4-10
4.3.4	Managing IMAP Samplers	4-11
4.3.4.1	Creating an IMAP Sampler	4-11
4.3.4.2	Modifying or Removing an IMAP Sampler	4-12
4.3.5	Managing SMTP Samplers	4-13
4.3.5.1	Creating an SMTP Sampler	4-13
4.3.5.2	Modifying or Removing an SMTP Sampler	4-14
4.3.6	Managing FTP Samplers	4-15
4.3.6.1	Creating an FTP Sampler	4-16
4.3.6.2	Modifying or Removing an FTP Sampler	4-17
4.3.7	Managing LDAP Samplers	4-17
4.3.7.1	Creating an LDAP Sampler	4-18
4.3.7.2	Modifying or Removing an LDAP Sampler	4-19
4.3.8	Managing DNS Samplers	4-20
4.3.8.1	Creating a DNS Sampler	4-20
4.3.8.2	Modifying or Removing a DNS Sampler	4-21

4.3.9	Managing RADIUS Samplers	4-22
4.3.9.1	Creating a RADIUS Sampler	4-23
4.3.9.2	Modifying or Removing a RADIUS Sampler	4-24
4.3.10	Managing Connection Samplers	4-24
4.3.10.1	Creating a Connection Sampler	4-25
4.3.10.2	Modifying or Removing a Connection Sampler	4-26
4.3.11	Managing Thresholds	4-26
4.3.11.1	Creating a Threshold	4-27
4.3.11.2	Modifying a Threshold	4-28
4.3.11.3	Removing a Threshold	4-28
4.3.11.4	Token Substitution in Threshold Action Parameter Strings ..	4-28
4.4	Managing Sampling Hosts	4-29
4.4.1	Enabling or Disabling Sampling Hosts	4-30
4.4.2	Removing Sampling Hosts	4-30
4.4.3	Shutting Down Sampling Hosts	4-30
4.4.4	Setting a Sampling Host Access Password	4-30
4.4.5	Setting Access Control for Sampling Host Connections	4-31
4.5	Monitoring Performance	4-31
4.5.1	Detail View	4-32
4.5.2	Summary View	4-32
4.6	Generating a Summary Report	4-32
4.7	Generating Detailed Reports	4-33
4.8	Performing Maintenance Functions	4-34
4.8.1	Setting Database Archiving Parameters	4-34
4.8.2	Enabling and Disabling Database Archiving	4-35
4.8.3	Setting Access Control for the Internet Monitor Administration Server	4-35
4.8.4	Managing Supported Sampler Types	4-36
4.8.4.1	Adding a New Sampler Type	4-36
4.8.4.2	Changing Sampler Type Ordering	4-37
4.8.4.3	Modifying or Removing a Sampler Type	4-38

5 Using the Sampler Extension Framework

5.1	Using the Example Web Sampler	5-1
5.2	Accessing API Documentation	5-1
5.3	Writing New Sampler Types	5-1
5.3.1	Establish the Build Environment	5-2
5.3.2	Create the Sampler Class	5-2
5.3.3	Create the Sampler Configuration Class	5-3
5.3.4	Create the Sampler User Interface Bean	5-4
5.3.5	Create the Sampler Management JSP	5-5
5.3.6	Build and Install the New Sampler Type	5-5
5.3.7	Register the New Sampler Type with the Internet Monitor	5-6

Index

Examples

3-1	Lines Added to the Properties File for Oracle 8i Enterprise Edition Database	3-15
-----	---	------

Figures

1-1	Internet Monitor Architecture	1-2
1-2	Performance Monitor Sampler Graph	1-5
1-3	Live Monitor Summary View	1-5
1-4	Sample Historical Report (Part 1)	1-7
1-5	Sample Historical Report (Part 2)	1-7
1-6	Sample Historical Report (Part 3)	1-8
1-7	Sample Summary Report	1-9
4-1	Internet Monitor Main Menu	4-1
4-2	Define Sampling Parameters Menu	4-2

Tables

3-1	Default Threshold Values	3-8
3-2	Contents of Internet Monitor Properties File	3-13
3-3	Default Values for PostgreSQL and Oracle 8i Databases	3-15
3-4	SampleReceived Message Properties	3-16
3-5	SampleReceived Message Body Properties	3-17
3-6	ThresholdChanged Message Properties	3-18
3-7	ThresholdChanged Message Body Properties	3-18
4-1	Default Port Numbers	4-3
4-2	HTTP Sampler Menu Fields	4-4
4-3	NNTP Sampler Menu Fields	4-6
4-4	POP Sampler Menu Fields	4-9
4-5	IMAP Sampler Menu Fields	4-11
4-6	SMTP Sampler Menu Fields	4-13
4-7	FTP Sampler Menu Fields	4-15
4-8	LDAP Sampler Menu Fields	4-18
4-9	DNS Sampler Menu Fields	4-20
4-10	RADIUS Sampler Menu Fields	4-22
4-11	Connection Sampler Menu Fields	4-24
4-12	Thresholds Menu Fields	4-26
4-13	Threshold Action Substitution Tokens	4-29
4-14	Summary Report Information	4-32
4-15	Detailed Report Generation Options	4-33
4-16	Sampler Type Menu Fields	4-36

About This Manual

This manual describes how to install, configure, and use the Internet Monitor software.

Audience

This manual is intended for the system administrator responsible for configuring Internet Monitor software on Tru64™ UNIX.

Organization

This manual consists of the following chapters:

<i>Chapter 1</i>	Provides an introduction to the Internet Monitor software.
<i>Chapter 2</i>	Describes how to install the Internet Monitor software.
<i>Chapter 3</i>	Provides tips on how to deploy the Internet Monitor software in your environment.
<i>Chapter 4</i>	Describes how to administer and configure the Internet Monitor software.
<i>Chapter 5</i>	Describes how to create Java classes and Java server pages that allow a new service type to be configured and monitored.

Related Documentation

You can also access the Documentation Bookshelf on the Internet Express CD-ROM. The documentation is available in the following formats:

- HTML
- PostScript
- Portable Document Format (PDF)

The Internet Express Documentation Bookshelf provides access to the following documents:

- *Release Notes* — This manual includes release notes for Internet Express.
- *Read This First* — This manual describes the contents of the kit.
- *Installation Guide* — This manual describes how to install the administration software and Internet Express software provided on the Internet Express for Tru64 UNIX CD-ROM.
- *Administration Guide* — This manual contains information on how to use the Administration utility to perform day-to-day maintenance tasks on a Tru64 UNIX system. When you run the Administration utility in a Web browser, this manual is linked to the utility to provide online help.
- *Secure Web Server Administration Guide* — This manual describes how to use the Secure Web Server Administration utility.
- *Internet Services User's Guide* — This document explains how to get started with e-mail, the TIN news reader, and a Web browser using a character-cell terminal.
- *Internet Monitor Administrator's Guide* — This manual.

- *Master Index* — This manual provides a master index to important topics covered in the Internet Express documentation set.
- *QuickSpecs* — This document is a specification of the Internet Express product.
- *Software Description and Licensing Terms* — This document describes the terms and conditions for software packaged with the current version of Internet Express.
- *Best Practices documents for Internet Express* — These documents provide you with recommended methods for performing specific tasks, rather than presenting all options.
Additional Best Practices are available at the Tru64 UNIX Publications Web site:
`http://www.tru64unix.compaq.com/docs/best_practices/`
- *Internet Express Reference Pages* — These reference pages are supplied with components that can be installed and managed using Internet Express.

Reading the Documentation

This section describes the different methods for accessing the Internet Express documentation.

Reading the Documentation Using the Administration Utility

After installation of the Secure Web Server subset (IAEAPCH), the Internet Express Documentation subset (IAEDOC), and the Internet Express Administration utility (IAEADM subset), you need access to the Administration utility for Internet Express (see the *Administration Guide*), so that you can read the documentation following the link from the Web page at

```
http://hostname.domain:8081
```

where *hostname.domain* is the host name and domain of the system running Internet Express.

Reading the Documentation Using the Public Web Server

You can also read the documentation without the Administration utility by using the public Web server (if you chose to configure one) to access the documentation index page at `http://hostname.domain/documents/bookshelf.html`.

If this URL does not work, verify that the Web server configuration file, `/usr/internet/httpd/admin/conf/httpd.conf`, contains the following line:

```
Alias /documents/ "/usr/internet/docs/IASS/"
```

Now, restart the Web server, using the following command:

```
# /sbin/init.d/httpd_public restart
```

The Internet Express documentation files are installed in the `/usr/internet/docs/IASS` directory.

You can access the Documentation Bookshelf installed on your system by entering the following URL (substituting the name of your system for *hostname*) in your browser:

```
http://hostname/documents/bookshelf.html
```

You can also read the installed documentation directly from the file system using a Web browser running on the same system by using the file URL:

```
file:/usr/internet/docs/IASS/bookshelf.html
```

Reading Reference Pages for Internet Express Components

Reference pages for Internet Express components are available in HTML format from the *Internet Express Reference Pages* index page. These HTML reference pages can be viewed using a Web browser.

Alternatively, you can view these reference pages from a command line in a terminal window if you modify the search path for the `man(1)` command.

The `man` command's search path needs to include the following directories for Internet Express component reference pages:

```
/usr/share/man
/usr/local/man
/usr/internet/pgsql/man
/usr/internet/openldap/man
/usr/news/man
/usr/local/samba/man
/usr/internet/httpd/man
/usr/opt/hpapache2/man
```

You can specify an alternative search path when entering the `man` command by using the `M` or `P` options; for example:

```
# man -M /usr/news/man active.5
```

You can also define the `man` command's `MANPATH` environment variable on the command line or in a file, such as your `.profile` file or `.login` file.

For example, suppose your `MANPATH` environment variable was defined to be the following:

```
/usr/share/man:/usr/dt/share/man:/usr/local/man
```

If you are using the `sh` or `ksh` shell, you could modify the `MANPATH` to add to the search path by adding the following:

```
# set MANPATH $MANPATH:/usr/internet/pgsql/man:/usr/internet/openldap/man:/usr/news/man: \
/usr/local/samba/man:/usr/internet/httpd/man:/usr/opt/hpapache2/man

# export MANPATH
```

If you are using the `csh` shell, you would use a command line like the following:

```
# setenv MANPATH $MANPATH:/usr/internet/pgsql/man:/usr/internet/openldap/man: \
/usr/news/man:/usr/local/samba/man:/usr/internet/httpd/man:/usr/opt/hpapache2/man
```

For details about defining reference page search paths, see `man(1)`.

Reading Documentation from the Internet Express CD-ROM

You can also access the Documentation Bookshelf on the Internet Express Installation and Documentation CD-ROM. The documentation is available in the following formats:

- HTML
- PostScript
- Portable Document Format (PDF)

On a Tru64 UNIX System

To read the documentation from the Internet Express for Tru64 UNIX CD-ROM on an AlphaServer™ system, follow these steps:

1. Log in to your system as root.

2. Insert and mount the Internet Express Installation and Documentation CD-ROM, replacing *drive* with the name of your CD-ROM drive:

```
# mount /dev/drive /mnt
```

Usually this will be:

```
# mount /dev/disk/cdrom0c /mnt
```

3. In a Web browser, open the Documentation Bookshelf file by entering the following URL:

```
file:/mnt/index.htm
```

4. Click on the book you want to open.

On a PC

To read the documentation from the Internet Express for Tru64 UNIX CD-ROM on a PC, follow these steps:

1. Insert the Internet Express Installation and Documentation CD-ROM into your PC's CD-ROM drive.

The Bookshelf page is automatically displayed in your browser.

If the Bookshelf does not appear, open the following URL, replacing *drive* with the letter of your CD-ROM drive:

```
file:drive:\index.htm
```

2. Click on the book you want to open.

Reading Software Component Documentation

The product kit also provides documentation (in ASCII text and HTML) for software components included with the product kit. This documentation is located in the `/usr/internet/docs` directory on the system where Internet Express is installed.

Reader's Comments

HP welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120. Attn: UBPG Publications, ZKO3-3/Y32
- Internet electronic mail: `readers_comment@zk3.dec.com`

A Reader's Comment form is located on your system in the following location:

```
/usr/doc/readers_comment.txt
```

Please include the following information with your comments:

The Tru64 UNIX Publications Group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate HP technical support office. Information provided with the software media explains how to send problem reports to HP.

Conventions

The following typographical conventions are used in this document:

%	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.
\$	
#	A number sign represents the superuser prompt.
% cat	Boldface type in interactive examples indicates typed user input.
<i>file</i>	Italic (slanted) type indicates variable values, placeholders, and function argument names.
cat(1)	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, <code>cat(1)</code> indicates that you can find information on the <code>cat</code> command in Section 1 of the reference pages.
Return	In an example, a key name enclosed in a box indicates that you press that key.
Ctrl/ <i>x</i>	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, Ctrl/C).

Introduction to the Internet Monitor

The Internet Monitor allows administrators to closely monitor the performance of mission-critical Internet services such as Web, E-mail, and news services. Automatic corrective actions can be initiated whenever performance of Internet services drops below administrator-defined thresholds. Historical reports and graphs of the performance of Internet services over time can be generated.

The Internet Monitor allows Internet service administrators to accomplish the following tasks:

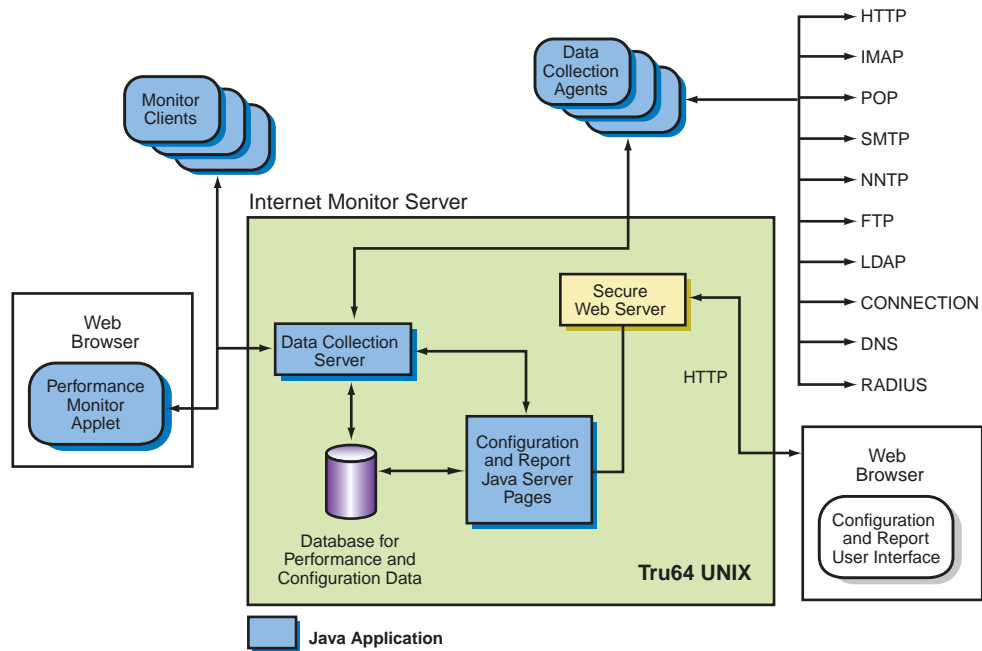
- Improve quality of service by spotting Internet service performance problems as soon as they occur, allowing timely corrective actions to be taken.
- Monitor compliance to performance-based service level agreements (SLAs) and generate periodic reports verifying this compliance. This capability is useful when users are paying for guaranteed levels of Internet service performance, such as in an Internet Service Provider (ISP) environment.
- Use historical performance data for resource planning tasks such as the sizing and purchase of new equipment.

The Internet Monitor is a component of HP's Internet Express product. It can be run either directly or from the Administration utility for Internet Express.

This chapter gives an overview of the Internet Monitor components (Figure 1-1). It covers the following topics:

- Data collection agents (Section 1.1)
- Data collection server (Section 1.2)
- Performance Monitor (Section 1.3)
- Historical report generation tools (Section 1.4)
- Getting started using the Internet Monitor (Section 1.5)

Figure 1–1: Internet Monitor Architecture



The Internet Monitor components include the following:

- **Data collection agents** — Applications that periodically access Internet services in the same manner that an actual user would, measure the response times for these client accesses, and report these response times back to the data collection server.
- **Data collection server** — An application that receives incoming feeds of performance data from data collection agents. The data collection server then performs automated response actions if administrator-defined performance thresholds are crossed, passes performance data to any monitoring clients that have requested it, and archives the performance data for use in historical report generation.
The data collection server can run on any Tru64 UNIX machine on the network.
- **Performance Monitor** — Allows real-time graphical monitoring of Internet service performance.
- **Historical report generation tools** — Allow reports and graphs of historical performance data to be generated.

The following sections provide details on these components.

1.1 Data Collection Agents

Data collection agents are responsible for periodically accessing Internet services and sending the response times for these operations to the central data collection server.

A data collection agent is a multithreaded Java application. An Internet services administrator typically deploys one or more of these agents on hosts at the edges of the network. This allows performance problems caused by any part of the network's infrastructure (network, system, or server application) to be detected.

Data collection agents can run on any UNIX or Windows based system with a Java runtime environment. HP packages agent software with a Java-based installation program, available for download from the Web-based configuration user interface. See Section 2.4 for downloading instructions.

For each agent, one or more samplers can be associated. A sampler is an object that defines a set of sampling operations an agent performs while measuring the total elapsed time it takes for the set of operations to complete. For example, an HTTP sampler might provide support to perform the following set of operations:

- Connect to the Web server `http://www.host.domain`
- Get the Web page `/index.html`
- Get the Web page `/products/prod1.html`
- Close the connection

By default, the Internet Monitor supports samplers for the following protocols:

- HTTP
- NNTP
- POP
- IMAP
- SMTP
- FTP
- LDAP
- DNS
- A basic connectivity sampler that measures the performance of connections to an arbitrary host and port

In addition to these sampler types that are supported by default, you can specify that the Internet Monitor monitor additional networking services. First you must create a number of Java classes and Java server pages that allow the new service type to be configured and monitored. These procedures are described in Chapter 5. You then use the Add Sampler Type menu to make the Internet Monitor aware of the new service. See Section 4.8.4.1.

Each sampler can perform sequences of operations that are common to clients that use that particular protocol. The data collection agent is capable of running several sampler objects simultaneously. For instance, an agent could measure HTTP GET performance by running an HTTP sampler configured to perform a GET operation every five minutes and measure IMAP performance by running a sampler configured to download 10 E-mail messages every 10 minutes. The same agent could also be simultaneously running other samplers configured to access LDAP, POP, or other supported Internet servers.

Data collection agents will normally be installed on machines other than the one upon which Internet Express software is installed.

The data collection agent passes the following information to the data collection server each time it attempts to access a sampler:

- Name of the data collection agent
- Name of the sampler
- The amount of time that it took to complete the operations specified for the sampler
- The number of bytes transferred
- The status code returned by the server
- The status message returned by the server
- Whether or not the server was accessible
- Whether the server returned an error code when the operation was attempted

1.2 Data Collection Server

The data collection server is a multithreaded standalone Java application. It typically runs on the same system as the main Internet Express installation but can run on any other Tru64 UNIX system if desired. It is responsible for a number of functions:

- Communicating configuration information to data collection agents
- Receiving feeds of performance information from data collection agents
- Performing any predefined actions if performance thresholds are crossed
- Storing performance information in a historical database
- Passing performance information to monitor clients that request it
- Providing current configuration information to configuration clients and processing configuration change requests from these clients

1.3 Performance Monitor

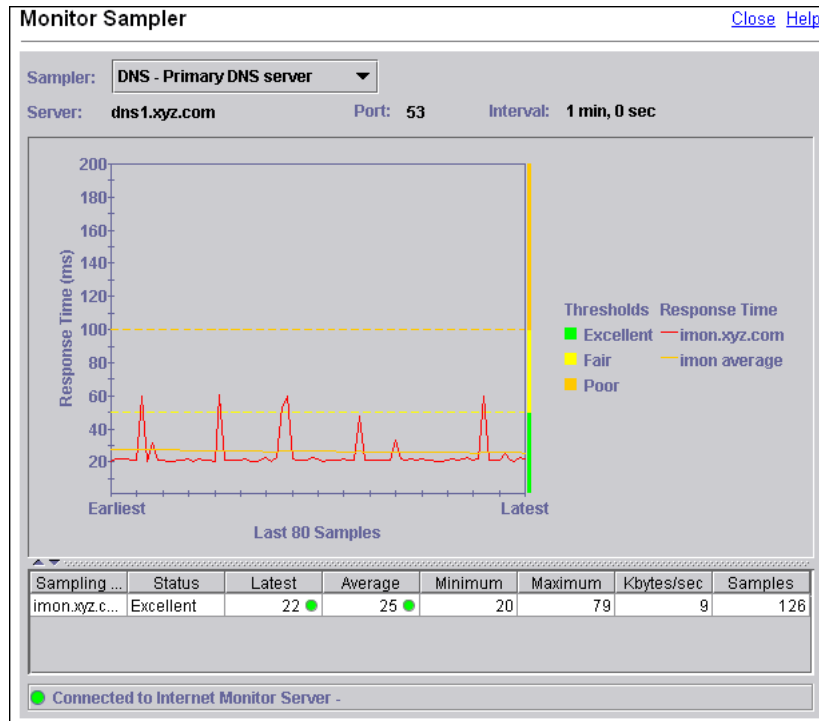
The Performance Monitor shows a graph of the current performance for a sampler over time.

There are two methods for running the Performance Monitor:

- As an applet within a browser window. Use this method by choosing Monitor Performance from the Internet Monitor menu. Section 4.5 describes how to access the Performance Monitor from within the Internet Monitor user interface.
- As a standalone application run outside of the Internet Monitor. To use the standalone method, you must first install the Performance Monitor application, as described in Section 2.5.

Figure 1–2 shows a monitor sampler graph generated from the Performance Monitor application.

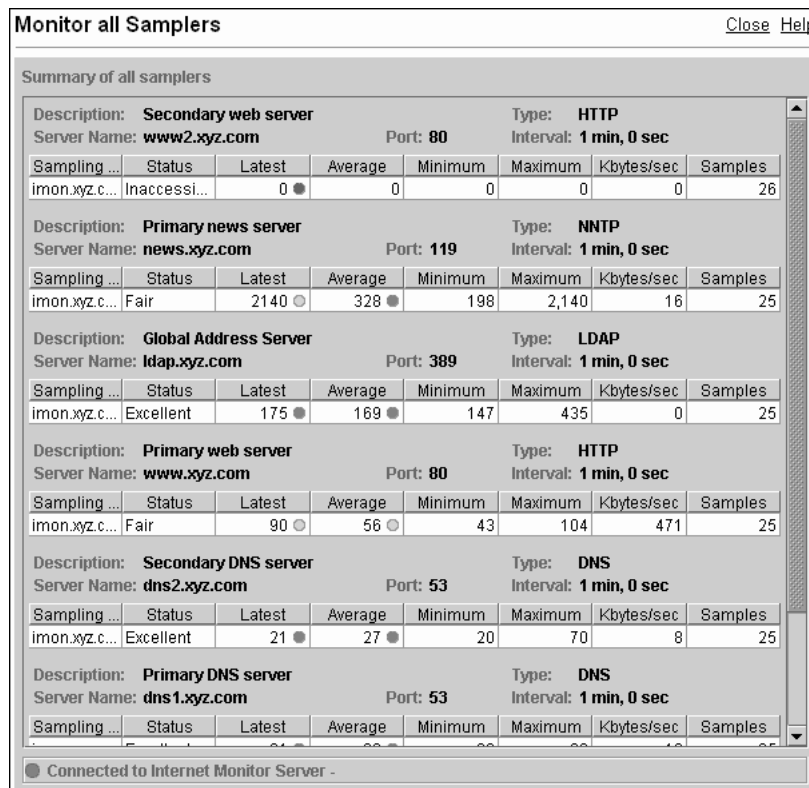
Figure 1–2: Performance Monitor Sampler Graph



The graph is updated as new performance information is received.

A summary window (Figure 1–3) shows the latest continually updated performance data for all samplers in a single window.

Figure 1–3: Live Monitor Summary View



1.4 Historical Report Generation Tools

The Internet Monitor provides report generation tools that allow administrators to review the past performance of their Internet servers. The tools are accessible from the Administration utility for Internet Express and allow the administrator to specify:

- Samplers on which to report
- List of agents on which to report for a given sampler (defaults to all agents)
- Reporting period

For each sampler, the information reported can include the following:

- Name and description of the sampler (host name, type, and port of the server being polled, description of objects being retrieved from the server, polling interval, and so on)
- Number of samples taken during the time period
- Timestamp of earliest and latest samples
- Low, high, and average response times
- Average byte count and throughput
- Number and percentage of samples where the polled server was inaccessible
- Number and percentage of samples where the polled server returned an error
- Number and percentage of samples at each threshold level that the administrator has defined
- Precise details on periods of service inaccessibility
- Precise details on service errors
- Breakdown of service performance over time throughout the reporting period

For a given sampler, the preceding data can be presented for each data collection agent to which it is attached. Also, a summary report can be generated that presents the combined statistics for all data collection agents to which the sampler is attached.

Figure 1–4, Figure 1–5, and Figure 1–6 show an example detailed report of a mail server sampler.

Figure 1–4: Sample Historical Report (Part 1)

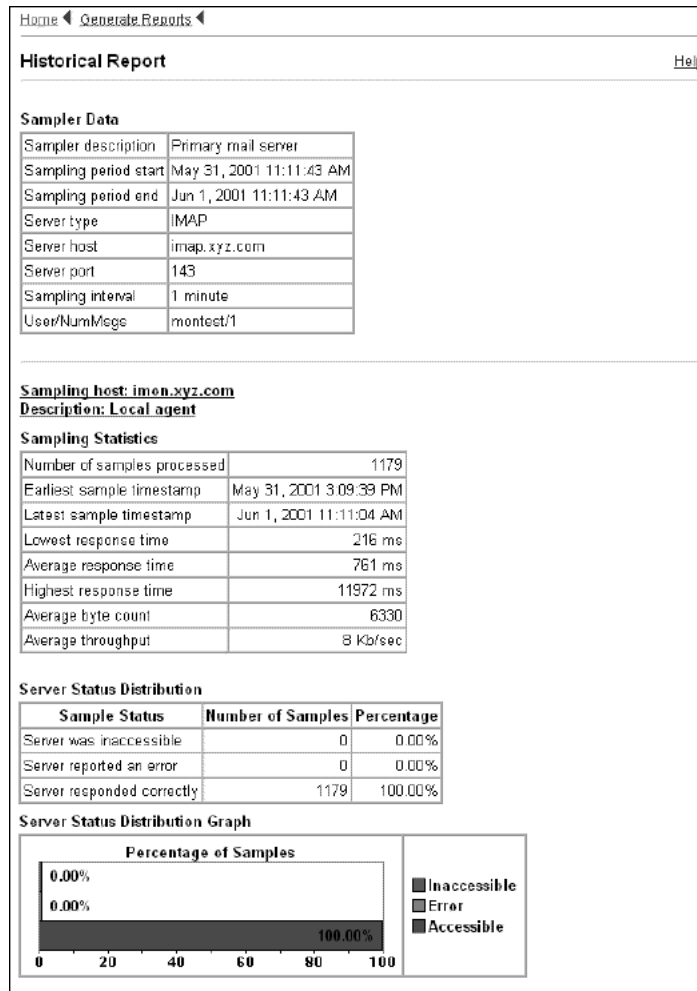


Figure 1–5: Sample Historical Report (Part 2)

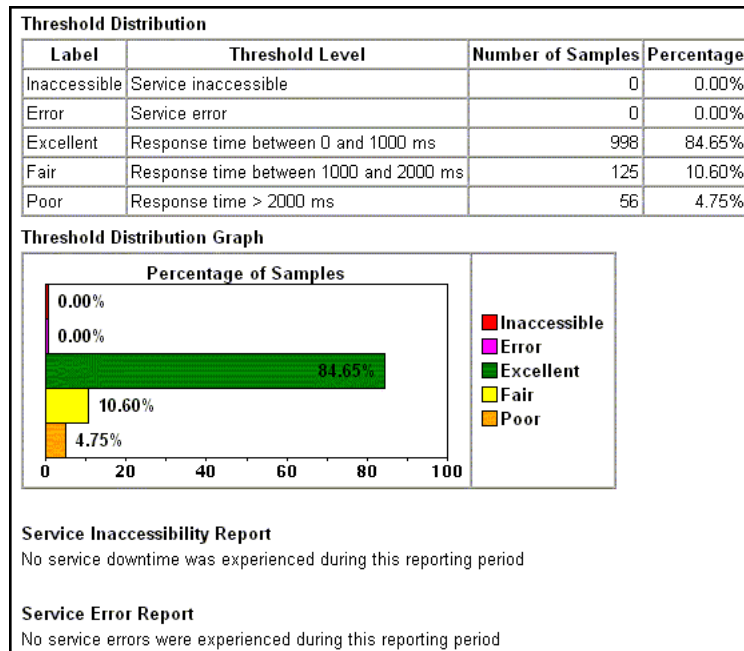
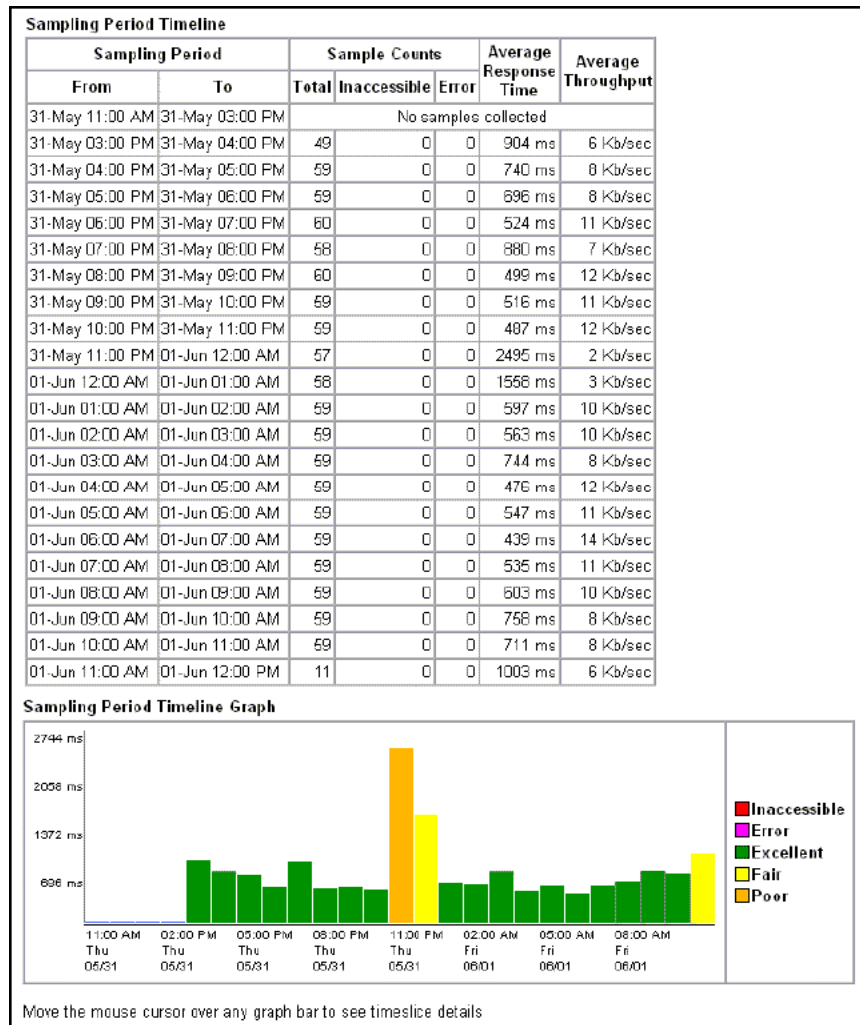


Figure 1–6: Sample Historical Report (Part 3)



You can also produce summary reports. The summary report provides a performance snapshot, displaying the most recently collected sampling data for each monitored service. Figure 1–7 shows an example of a summary report.

Figure 1–7: Sample Summary Report

Home ◀

Summary Report [Help](#)

Web servers				
Sampling Target	Last sampled	Response time	Status	Detailed reports
Primary web server	3:15:01 PM	50 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)
Secondary web server	3:16:39 PM	-	■ Inaccessible	Last 1 , 6 , 12 , 24 hour(s)

DNS servers				
Sampling Target	Last sampled	Response time	Status	Detailed reports
Primary DNS server	3:18:39 PM	20 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)
Secondary DNS server	3:19:08 PM	24 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)

LDAP directory servers				
Sampling Target	Last sampled	Response time	Status	Detailed reports
Global Address Server	3:15:19 PM	150 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)

IMAP servers				
Sampling Target	Last sampled	Response time	Status	Detailed reports
Primary mail server	3:05:05 PM	540 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)

News servers				
Sampling Target	Last sampled	Response time	Status	Detailed reports
Primary news server	2:58:20 PM	151 ms	■ Excellent	Last 1 , 6 , 12 , 24 hour(s)

Generated on Tue Jun 19 15:19:42 EDT 2001

1.5 Getting Started with the Internet Monitor

To begin using the Internet Monitor for the first time, follow these steps:

1. Install the Internet Monitor subsets on a Tru64 UNIX machine (Chapter 2).
2. Decide which systems on which the sampling hosts will be run (Section 3.2.1).
3. For each of the systems where sampling hosts will be run, install the agent software and start the agents (Section 2.4).
4. Create samplers for each of the Internet services that you want to monitor (Section 4.3). For some services, this may involve creating target (dummy) accounts (Section 3.3.6).
5. Optionally, create thresholds for each of the samplers (Section 3.4 and Section 4.3).
6. Use Perform Sampling from the Following Hosts section of the Create Sampler menu to attach the sampler to the sampling host (Section 4.3).
7. At this point, the samplers will begin actively collecting performance data. You can then monitor their performance in real time or generate historical reports based upon the collected performance data as needed. (See Section 4.5 and Section 4.7). You can also enable archiving to prevent your samples database from becoming too large over time (Section 4.8).

Installing the Internet Monitor

This chapter describes how to install the Internet Monitor software.

2.1 Prerequisites

The Internet Monitor depends on the Java 1.3.1 Software Development Kit (SDK) or later. The SDK must be installed before you install the Internet Monitor software. The SDK for Tru64 UNIX can be downloaded from the following Web site:

<http://h18010.www1.hp.com/java/download/index.html>

The Java SDK subset also requires the OSFX11 nnn Basic X Environment subset, which is normally a required part of the Tru64 UNIX operating system installation unless you do not have a graphics card in your system. In this case, the Basic X Environment subset is optional. The Java SDK subset does not enforce that dependency, but the Java virtual machine will not run without it.

2.2 Choosing an Installation Interface

You can use either a browser-based interface or a command-line interface to perform the Internet Monitor installation.

You can use the Internet Express installation procedure (`ix_install`) to install some or all Internet Express components, including Internet Monitor. The installation procedure presents a series of prompts for determining which of the following interfaces you want to use to continue the installation:

- A new Web browser (either local or remote)
- An existing Web browser (either local or remote)
- No browser (command-line interface)

For more information about Internet Express installation, see the *Installation Guide*.

This chapter shows the command-line procedure for installing Internet Monitor.

2.3 Installing the Internet Monitor

The Internet Monitor can be installed on any Tru64 UNIX machine. It does not have to be installed on the same machine as the Internet servers that will be sampled or on the same machine as any data collection agent that will be doing the sampling. Although the Internet Monitor components are not particularly bandwidth or CPU-intensive, administrators concerned about the impact on the performance of other applications on the machine can choose to install the Internet Monitor on a Tru64 UNIX machine that does not have any other performance-sensitive applications running on it.

The Internet Monitor installation requires that you install the necessary Internet Express and Internet Monitor subsets in order.

To install the Internet Monitor software:

1. Log in as `root` and change your working directory to the location of the Internet Monitor components.

2. Enter the following commands to install the required Internet Express subsets:
 - a. `# setld -1 . IAEAPCH600`
The IAEAPCH subset prompts you to configure a Public Web server for general use.
 - b. If you answer yes to this question, the Secure Web Server 1.3 (*powered by Apache 1.3*) subset will create an instance of itself that will operate on the default HTTP port of 80. A public instance is not required for the Internet Monitor to operate.
 - c. Enter the following command to install the required database management system:
`# setld -1 . IAEP SQL600`
The PostgreSQL (IAEP SQL600) subset asks you to specify a location for the database. This database is used to store the collected performance data and will change frequently and grow in size. The selected directory should probably not be part of the `/usr` or `/var` file systems for optimum performance.
 - d. Enter the location for the database.
3. Enter the following commands to install the required Internet Monitor subsets:
 - a. `# setld -1 . IAEMOND600`
 - b. `# setld -1 . IAEMON600`

When the installation completes, all services should be configured and running. The configuration interface can be accessed using a Web browser. The configuration interface Web server is listening on port 8086, and by default access is restricted to Web browsers on the local machine. To access the interface, enter a URL in the format `http://host.domain.name:8086` into your Web browser.

2.4 Installing Agent Software

Before you can begin monitoring the performance of your Internet services, you must install the agent software on each machine that you would like to perform sampling operations (Section 4.4).

A data collection agent is installed by default as part of the Internet Monitor subset installation. Additional agents can be installed on other machines as needed.

Agents can be installed on any UNIX or Windows-based system that has a Java Runtime Environment or Java Development Kit installed. The minimum version is 1.3.1. Section 2.1 describes how to obtain the Java software.

If it is not present on your system, you should install one of these Java kits and change your current `PATH` variable so that it contains the directory where the `java` binary is installed.

You must first configure the Internet Monitor administration user interface to allow access from remote browsers. For instructions on how to do this, see Section 4.8.3.

To download and install agent software, follow these steps:

1. Click on this link: `/class/agent.jar`

Note

Alternately, you can use FTP or some other method to download the agent installation file, `/usr/internet/monitor/web/class/agent.jar`, which is located on the machine

where the Internet Monitor was installed. If you use the FTP method, follow the instructions displayed by the agent installation program.

2. Choose a directory in which to install the agent software.
3. On the system on which you downloaded the agent software, set the environment variable CLASSPATH equal to agent.jar and run the command `java ConfigureAgent`.

- On a UNIX system, use syntax similar to the following:

```
# CLASSPATH=agent.jar java ConfigureAgent
```

- On a Windows system, use the following commands:

```
C:\> set CLASSPATH=agent.jar
C:\> java ConfigureAgent
```

The agent configuration program will attempt to connect to the data collection server and register the agent. If it succeeds, the agent will appear in the list of available sampling hosts whenever a sampler is created or modified. If the configuration program is unable to connect to the data collection server, the configuration will fail. In this case, you must correct the problem and run the configuration program again.

Note

If the Create or Modify Sampler page is open when you are installing the agent software, you will need to refresh or reload the page to see the newly configured agent in the sampling hosts list.

2.5 Installing the Performance Monitor Application

The Performance Monitor application requires Java Version 1.3.1 or later.

To download and install the Performance Monitor application, follow these steps:

1. Click on this link: [/class/monitorapp.jar](#)

Note

Alternately, you can use FTP or some other method to download the installation file (`/usr/internet/monitor/class/monitorapp.jar`), which is located on the machine where the Internet Monitor was installed. If you use the FTP method, follow the instructions displayed by the agent installation program.

2. Choose a directory in which to install the Performance Monitor application software.
3. To run the application on a UNIX system, use syntax similar to the following:

```
# /usr/opt/java122/bin/java -jar path_to_jar_file/monitorapp.jar
```

To run the application on a Windows system, double click on or open the `monitorapp.jar` icon in Windows Explorer.

2.6 Configuring the Agent to Restart Automatically on a UNIX System

The data collection agent installation procedure creates a script that can be used to force an agent to start automatically whenever the system reboots. The following instructions show how to install this script for Tru64 UNIX. For other versions of UNIX, consult your operating system documentation.

The following instructions require an installed agent in a directory called `/usr/agent`; substitute your actual agent installation directory, if appropriate.

During the installation procedure, you will be asked to specify a user for the agent. Ensure that the directory for the agent is readable and writable by that user, and make sure that the files in that directory are readable by that user.

1. Log in as the `root` user.
2. Type the following commands:

```
# ln -s /usr/agent/monitor_agent \  
/sbin/init.d/monitor_agent  
  
# ln -s /sbin/init.d/monitor_agent \  
/sbin/rc3.d/S79monitor_agent
```

You can then start the agent manually with the following command:

```
# /sbin/init.d/monitor_agent start
```

You can stop the agent manually with the following command:

```
# /sbin/init.d/monitor_agent stop
```

The agent will start automatically whenever the machine reboots. Any agent error messages or output will be written to a file called `agent.log` in the agent installation directory.

Deployment Guidelines

This chapter provides guidelines for addressing the following concerns with the Internet Monitor software in your environment:

- Sampler database sizing guidelines (Section 3.1)
- Data collection agent deployment guidelines (Section 3.2)
- Sampler configuration guidelines (Section 3.3)
- Threshold configuration guidelines (Section 3.4)
- Security guidelines (Section 3.5)
- Configuring the Internet Monitor for use in a firewalled environment (Section 3.6)
- Configuring the Internet Monitor to use alternate databases (Section 3.7)
- Using the Java Message Service (Section 3.8)

3.1 Sampler Database Sizing Guidelines

When the data collection server receives samples from data collection agents, these samples are stored in a local database, so that they are available for use by historical report generation tools. Depending upon how many samplers are running and how often they are sampling, this database can fill the disk over time.

Each sample written to the database consumes approximately 175 bytes. Therefore, a sampler that samples an Internet service every five minutes causes the sampler database to grow in size by about 50 kilobytes per day, or approximately 1.5 megabytes per month.

To ensure adequate disk space for the sampler database, you must estimate the disk space required for the number of samplers that will be deployed and how frequently they will be sampling. The Perform Maintenance Functions option on the Internet Monitor administration utility allows you to periodically remove old records from the samples database and write them to an archive file, which can then be removed or backed up to tape. This practice will prevent the samples database from filling the disk over time.

Section 4.8 describes the Perform Maintenance Functions option.

3.2 Data Collection Agent Deployment Guidelines

The following sections provide guidelines for deploying the data collection agent.

3.2.1 Determining the Location for Installation of the Data Collection Agent

Data collection agents can be deployed on any UNIX or Windows-based machine that has a Java runtime environment (minimum Version 1.1.8). Only one data collection agent can be run on each machine. Multiple samplers can be attached to each data collection agent, so you do not need to run more than one data collection agent on a given machine.

Data collection agents access Internet services in the same way that actual users do. By experiencing the same potential network, system, and application

performance problems that users might experience, agents provide an accurate picture of the Internet service performance that those users are experiencing.

For this reason, data collection agents should be deployed on machines in the same part of the network where users are accessing the Internet servers being monitored. Some recommended locations include the following:

- On or near a dial-in access server accessed by users to connect to and then access Internet services such as E-mail and news.
- At or near a network boundary, to measure the performance of Internet services being accessed by users outside your network.
- On a machine in any part of the network where many users are accessing Internet services.

3.2.2 Determining the Number of Agents to Deploy

Because one data collection agent can run multiple samplers, small networks where most users see similar performance regardless of where on the network they are located probably require only one data collection agent to be deployed.

In larger, more complex networks, where users accessing Internet services are likely to see dramatically different performance depending upon where in the network they are located, you should deploy more agents. For instance, if a company has two different remote locations and users from both are accessing the same Internet servers, you should deploy a data collection agent in each location so the service performance experienced by each distinct user group can be monitored.

You can also deploy multiple data collection agents to spread the sampling load among them. Data collection agents are lightweight applications that generally have little impact on the performance of the systems where they are running. However, if large numbers of samplers that perform frequent sampling operations are attached to one data collection agent, the data collection agent could adversely affect the performance of other applications on the system. In this case, more data collection agents can be deployed on nearby machines, and the attached samplers can be distributed among them.

3.2.3 Autostarting Agents After Installation

You will probably want to configure the systems where data collection agents are installed to automatically start the agents when these systems are rebooted. The configuration steps vary by operating system. Section 2.6 describes how to do this for a UNIX system.

Consult the system administration documentation for the operating systems.

3.3 Sampler Configuration Guidelines

This section provides the following guidelines for configuring samplers:

- Determining a sampler interval (Section 3.3.1)
- Determining the data to be retrieved by a sampler (Section 3.3.2)
- HTTP sampler deployment (Section 3.3.3)
- NNTP sampler deployment (Section 3.3.4)
- POP and IMAP sampler deployment (Section 3.3.5)
- SMTP sampler deployment (Section 3.3.7)
- Creating target users for the SMTP, POP and IMAP samplers (Section 3.3.6)
- FTP sampler deployment (Section 3.3.8)

- RADIUS sampler deployment (Section 3.3.9)
- Connection sampler deployment (Section 3.3.10)

3.3.1 Determining a Sampling Interval

The Internet Monitor is a monitoring tool, not a tool for load testing your Internet services. Sampling Internet services too frequently could adversely impact the performance of the service being sampled as well as that of the machines running the data collection agent and Internet Monitor. It will also cause the database where sample performance data is stored to fill up more quickly. For these reasons, you should choose sampling intervals of 10 seconds or more. For most sites, intervals of five minutes or more are probably more appropriate.

3.3.2 Determining the Data to be Retrieved by a Sampler

Most samplers retrieve data such as Web pages, mail messages, and so on from an Internet server. For consistent performance measurements, the same data should be retrieved each time the Internet server is sampled. The following guidelines address this requirement for each sampler type.

3.3.3 HTTP Sampler Deployment Guidelines

For HTTP samplers, choose documents to sample that are not likely to change in size or to be removed or renamed frequently. Specifying a URI of “/” will always cause the sampler to retrieve a Web server’s root document. Because this document always exists and is the starting point for most users that access a Web site, it makes a good choice when deciding what URIs an HTTP sampler will access.

3.3.4 NNTP Sampler Deployment Guidelines

The NNTP sampler requires a target newsgroup on the target machine. The NNTP sampler queries the target newsgroup during each sample, downloading the list of available articles and then fetching the header of each one. Because the content of most public newsgroups changes frequently, sampling a public newsgroup is likely to give inconsistent performance results. (The newsgroup might contain five messages one day and 500 messages the next day.)

This section describes a method of creating a target newsgroup using the InterNetNews (INN) news server provided with Internet Express. See the *Internet Express Administration Guide* for more information on configuring InterNetNews.

To create a target newsgroup, use the following procedure:

1. Create a newsgroup (Section 3.3.4.1)
2. Limit export of a newsgroup so new messages will not be propagated to other Usenet feeds (Section 3.3.4.2)
3. Change the expiration handling of the target newsgroup so that the content is always retained (not expired) (Section 3.3.4.3)
4. Post a number of sample messages to the newsgroup (Section 3.3.4.4)

3.3.4.1 Creating a Newsgroup

You can use the Administration utility for Internet Express to create a newsgroup. Under Manage Components, choose InterNetNews.

To create a newsgroup from the Tru64 UNIX command line, use the `ctlinnd` command. For example:

```
# ctlinnd in-group local.sampler y sampleradmin
```

In this example, *local.sampler* is the name of the newsgroup to be created, and *sampleradmin* is the E-mail address of the group creator.

For details on the `ctlinnd` command, see `ctlinnd(8)`.

3.3.4.2 Limiting Export of a Newsgroup

With the Internet Express news package, any newsgroup in the `local` hierarchy is not exported to other news feeds.

Limiting the export of a newsgroup can be done by modifying the `newsfeeds` file. See `newsfeeds(5)` for more information.

3.3.4.3 Modifying Article Expiration Definitions for the Target Newsgroup

You should modify the expiration definitions for the `InterNetNews` newsgroup, so that the articles in the group will not expire.

You can use the Administration utility for Internet Express to modify the expiration definitions for a newsgroup, using these steps:

1. Under Manage Components, choose `InterNetNews`.
2. On the `InterNetNews` menu, choose `Modify Article Expiration Definitions`.
3. Set the retention on the group to indefinite.

To manually modify the expiration handling of a newsgroup, see `expirectl(5)`.

3.3.4.4 Posting Sample Messages to the Target Newsgroup

Using any news reader client, post a number of messages to the target group. The number of messages present in the group will affect each sample. Five to 20 messages is a reasonable number of messages to have present in the newsgroup, although no limit is imposed by the Internet Monitor system.

3.3.5 POP and IMAP Sampler Deployment Guidelines

POP and IMAP samplers measure the time to download messages from the `INBOX` folder of an E-mail user. Because the content of users' folders changes frequently and unpredictably, set up a dummy mail account and populate it with dummy mail messages. The number and size of the mail messages should approximately equal the average values of these figures for your user base. See Section 3.3.6.

Because many POP servers implement mechanisms for preventing simultaneous access to a user's account by multiple clients, no more than one agent should be configured to sample a given POP account. If multiple agents are configured to sample the same POP account, some agents might report error samples when they are unable to access the POP account because it is currently locked by another agent.

3.3.6 Creating Target User Accounts for SMTP, POP, and IMAP Samplers

This section describes how to create target user accounts for the SMTP, POP, or IMAP samplers.

The SMTP, POP, and IMAP samplers require a user account on the target system. The SMTP sampler sends an E-mail message to the account during each sample. The POP and IMAP samplers require a valid E-mail account on the target system to query during each sample.

If you are using a mail system other than the ones described, consult that mail system's documentation for creating a user.

Creating a target user is accomplished by these steps:

- Create a UNIX user account for the target user (Section 3.3.6.1)
- Configure E-mail for the target user (Section 3.3.6.2)
- Populate a target user account with test messages (Section 3.3.6.3)
- Dispose of any new messages (Section 3.3.6.4)
- Improve security for target user accounts (Section 3.3.6.5)

3.3.6.1 Creating a UNIX Target User Account

You should create a user account for the target user. This account can use any valid name. For security reasons, the account should be allocated a unique user or group ID. This account can be created using the Internet Express Administration utility interface or the UNIX system tools.

For more information on creating a user account with the Internet Express Administration utility interface, see the *Internet Express Administration Guide*.

Refer to `adduser(8)` for more details on creating a user with UNIX system tools.

If the user account password was not set while creating the user account, use the `passwd(1)` command to set the account password to a known value.

3.3.6.2 Configuring E-Mail for the Target User Account

The target user account will need to receive E-mail.

You should send a test message to the account to verify that the account is properly receiving and storing E-mail messages.

Certain E-mail systems require additional configuration steps to activate the user account so that it will receive E-mail. For example, Cyrus IMAP requires a user account be configured before it will accept mail for that user.

If `sendmail` is being used (the default Tru64 UNIX mail transport system), the user may need to be added to the `/var/adm/sendmail/local.users` file. After modifying this file, be sure to restart `sendmail` as documented in the comments within the file.

3.3.6.3 Populating a Target User Account with Test Messages

Send a number of test E-mail messages to the target user. The number of messages is arbitrary but should probably be five to 20 messages. Because the size of the message influences the sampling, you should vary the size of the message body so the messages reflect a normal user's mail. The number of messages to be downloaded by the sampler is specified when a sampler is created.

Verify that the E-mail has been received and is stored in the appropriate mail pool.

3.3.6.4 Disposing of Any New SMTP Messages

The SMTP sampler sends an E-mail message to the target account each time a sample is performed. If steps are not taken to dispose of these arriving messages, the mail spool for the target user will continue to grow, consuming valuable disk resources (as well as affecting the other samplers that use this account).

The SMTP sampler sends an E-mail message with the Subject: `Internet Monitor test message`.

Two mechanisms will be presented for automatically disposing of arriving E-mail. For each method to work properly, the user's `.forward` file must be correctly

handled. If the `.forward` file is not being invoked, consult your mail transport's documentation.

You should use the `mailx` command with the verbose option (`-v`) on the target machine. This option causes the `mailx` command to output the SMTP commands and responses and can often provide help if problems are encountered. For example, you would enter the following command:

```
# mailx -v username
```

3.3.6.4.1 Using the `slocal` Command to Filter Incoming E-Mail

The `slocal` command can be used to filter incoming E-mail. The command can be found in the `OSFMH` optional subset. To use the command, create two files in the target user's home directory. These files must be owned by the user. To assure proper ownership, use the `su - username` command to become the user prior to creating the files.

1. Create a file in the user's home directory called `.maildelivery` containing the following one line:

```
* - destroy A -
```

This line directs the `slocal` command to destroy all messages that are received. The entry can be tailored to destroy only the sampler messages as shown by the following line:

```
Subject "Internet Monitor test message" destroy A -
```

See `slocal(1)` for more information on the `.maildelivery` file syntax.

2. Create a file in the user's home directory called `.forward` containing the following one line:

```
"| /usr/lib/mh/slocal -user username"
```

3. Substitute your target account's user name for `username` in the example. The double quotes in the example are required.

The `.forward` file enables the `slocal` processing. To disable the processing, remove or rename the file.

3.3.6.4.2 Using the `procmail` Command to Filter Incoming E-Mail

The `procmail` command can be used to filter incoming E-mail. The command can be found in the optional `IAEPROC` subset of the Internet Express kit.

To use this command, create two files in the target user's home directory. These files must be owned by the user. One method to verify proper ownership is to use the `su - username` command to become the user prior to creating the files.

1. Create a file in the user's home directory called `.procmailrc` containing the lines:

```
:0  
/dev/null
```

These lines direct `procmail` to destroy all messages that are received. The entry can be tailored to destroy only the sampler messages as shown by the following lines:

```
:0  
* ^Subject:.*Internet Monitor test message  
/dev/null
```

See `procmail(1)` for more information on the `.procmailrc` file syntax.

2. Create a file in the user's home directory called `.forward`, containing the following one line:

```
" | /usr/bin/procmail"
```

The double quotes in the example are required.

The `.forward` file enables the `procmail` processing. To disable the processing, remove or rename the file.

3.3.6.5 Improving Security for Target User Accounts

For the samplers to operate, a target account must be a valid login account with a password. The following methods can reduce the risk associated with these target accounts.

- Create a UNIX group that will be used only for the target accounts.
- When creating the accounts, do not share the user ID with any account that is not a target test account.
- After performing the other configurations required for the samplers to operate, and verifying that samplers are operating properly, change the login shell of the target accounts. Changing the login shell to `/bin/true` will prevent login from the command line but will not interfere with the operation of the samplers.

3.3.7 SMTP Sampler Deployment Guidelines

The SMTP sampler sends a mail message to the specified recipient via the specified SMTP server. Because the SMTP sampler will be repeating this process continuously, the sampler messages sent to the recipient E-mail address will accumulate over time.

For this reason you should create a dummy user account to receive SMTP sampler mail messages. This user account can be set to automatically delete SMTP sampler mail messages as they arrive. See Section 3.3.6.4.

3.3.8 FTP Sampler Deployment Guidelines

The FTP sampler connects to an FTP server and downloads documents or performs directory operations. To achieve consistent performance results, you should choose directories and files that are unlikely to change in size, to be removed from the server, or to be renamed.

3.3.9 RADIUS Sampler Deployment Guidelines

The administrator should create a dummy user account with minimal privileges that can be used as an authentication target for RADIUS sampling.

Once the dummy user account is created, you must configure the RADIUS server to allow connections from the data collection agents that will be sampling it. For instance, if the Interlink AAA RADIUS Server that ships with Internet Express is being used, edit the `/usr/private/etc/raddb/clients` file and add a line like the following:

```
clienthost.xyz.com thesecret type=Merit:PROXY
```

where *clienthost.xyz.com* is the host where the data collection agent will be running and *thesecret* is the shared secret that must be supplied when the RADIUS sampler is being configured.

3.3.10 Connection Sampler Deployment Guidelines

The Connection sampler can be used to measure the amount of time required to open and then immediately close a network connection to an arbitrary host and port. This capability is useful in the following situations:

- When the administrators primary concern is determining whether a remote server is accessible or not, as opposed to measuring its performance.
- When the administrators primary concern is determining whether a remote system is accessible or not, and the remote system is not running any of the Internet server types (HTTP, NNTP, and so on) supported by the Internet Monitor.
- When the administrators primary concern is measuring the speed of the network connection between the agent and the remote system that it connects to, with the least possible amount of time spent by the remote server processing the network request.
- When the administrators primary concern is determining whether a server of a type not currently supported by the Internet Monitor (such as telnet) is accessible.

3.4 Threshold Configuration Guidelines

The process of defining threshold actions triggered when Internet service performance drops below certain levels is detailed in Section 4.3.11.

When you define a new sampler, three thresholds are created and attached to each new sampler by default. These three default thresholds can be modified or deleted if desired, and new thresholds can also be added. The three default thresholds are shown in Table 3–1.

Table 3–1: Default Threshold Values

Label	Color	Type
Inaccessible	Red	Server Inaccessible
Error	Magenta	Service Error
Accessible	Green	Response Time > 0ms

Note these guidelines when defining thresholds:

- When setting response time thresholds, it is recommended that you create a base threshold with a response time of zero that will be applied if the response time of a sample does not exceed the other thresholds that have been established. For example, you could set the following thresholds for a Web server:

Label	Color	Response Time Boundary
Excellent	Green	0 ms
Fair	Yellow	2000 ms
Poor	Pink	5000 ms
Error	Magenta	Server Error
Inaccessible	Red	Server Inaccessible

- Use the Action Trigger field to specify how many consecutive samples must exceed a threshold boundary before the threshold action is triggered. This prevents isolated performance spikes from causing actions to be triggered.

Once a threshold action is triggered, it is not eligible to be triggered again until the action for a different threshold has been subsequently triggered.

- When specifying a system call threshold action, keep in mind that specified shell commands are executed by a process spawned by the data collection server, which runs as user `nsim`. Ensure that the `nsim` user has sufficient permission to perform whatever system call is specified.
- If you want a threshold action to perform several tasks (send an E-mail message, write a message to a log file, and restart a server, for example), write a script that performs these tasks and specify it as a system call threshold action.

3.5 Security Guidelines

Follow these security guidelines for Internet Monitor:

- System security

The data collection server and data collection agents should be installed on secure systems to prevent unauthorized access to these components.

- User interface security

By default, access to the Web-based administration interface is restricted to the Internet Express administration user. If desired, the Web server access controls can be modified to allow access by other users. Different access controls can be set up for access to the configuration, Performance Monitor, and historical report generation interfaces, allowing you to let different groups of users access each. These access controls can be set by modifying the configuration files of the Secure Web Server rooted at `/usr/internet/httpd/monitor_admin`.

- Agent access to the data collection server

When a data collection agent attempts to connect to the data collection server, the data collection server determines the host name of the connecting agent. The host name must be on the list of registered sampling hosts. Sampling hosts are registered when the agent configuration program is run on them and it successfully connects to the data collection server to perform the registration. If this sampling host name is not on the list, the connection is rejected.

This level of security is sufficient for most sites; however, the administrator can define an agent password through the Set Agent Password page, accessible from the Install Agent Software menu (Section 2.4). If this password is defined, connecting agents must supply the specified password in addition to connecting from a host that has been registered with the data collection server. The agent software installation package prompts for this password and will pass it to the data collection server whenever the data collection agent attempts to establish a connection.

3.6 Configuring the Internet Monitor for Use in a Firewalled Environment

When the data collection server is separated from data collection agents by a firewall, the following steps are necessary to enable communication between them:

1. The firewall and routing software must be properly configured so that network requests between the data collection server system and agent systems are routed through and screened by the firewall system. See your firewall documentation for more information on this step.
2. The data collection server system must be able to translate the IP addresses of the agent systems into fully qualified host names. Likewise, the agent systems must be able to translate the IP address of the data collection server system into a fully qualified host name. This step is accomplished by adding entries

for these addresses to the appropriate DNS servers or local host files. See your operating system's networking documentation for more information.

3. The data collection server must be configured to a known port for RMI communications. Edit the `/usr/internet/monitor/.properties` file on the system where the data collection server is installed and add the following line to the end of the file:

```
com.compaq.osis.ism.dcs.rmiPort=portNumber
```

where *portNumber* is an unused port number greater than 1024 on the data collection server system.

Restart the data collection server after modifying the properties file with the following command:

```
#!/sbin/init.d/nsim restart
```

4. When you install each agent, the installation process will ask whether you want to specify a nonarbitrary port for use in RMI communications between the agent and the data collection server. Specify an unused port on the agent system in response to this question. You do not have to specify the same port for each agent system, but it will make configuration of your firewall easier if you do so.
5. The data collection server must be configured to serve Java class files on a port other than 8086. The default port number for serving the Java class files is 8090. On the system where the data collection server is installed perform the following steps:

- a. Edit the `/sbin/init.d/nsim` file and remove the comment character (`#`) from the line:

```
#OPTIONS=-DAlternateJavaClassPort
```

- b. Edit the `/usr/internet/monitor/.properties` file and add the following line to the end of the file:

```
com.compaq.osis.ism.classPort=portNumber
```

where *portNumber* is an unused port number greater than 1024 and not 8086

- c. If a port number other than 8090 was used in Step 5b, edit the `/usr/internet/httpd/monitor_admin/conf/httpd.conf` file and replace the port 8090 reference in the lines `Listen 8090` and `<VirtualHost _default_:8090>` with the port number used in Step 5b.

6. For each agent that you have installed, configure your firewall to allow the following TCP communications:
 - Connections from any port on the agent system to the port on the data collection server system that you specified in Step 5. These connections are used by the agent to download Java class files from the Web Server on the data collection server system.
 - Connections from any port on the agent system to port 1098 on the data collection server system. These connections are used by the agent to obtain RMI registry information from the data collection server.
 - Connections from any port on the agent system to the port on the data collection server system that you specified in step 3. These connections are used for RMI communications initiated by the agent.
 - Connections from any port on the data collection server system to the port on the agent system that you specified in step 4. These connections are used for RMI communications initiated by the data collection server.

3.7 Configuring the Internet Monitor to Use Alternate Databases

By default, the Internet Monitor stores its configuration information and collected sampling data in PostgreSQL databases that are located on the Internet Monitor host. However, the Internet Monitor can be configured to alternatively use any other database that supports the Java Database Connectivity (JDBC) standard. The database can be installed on either the same machine as the Internet Monitor or on a different machine.

Use the following procedures to configure the Internet Monitor to use an alternate database:

- Install and configure the database product (Section 3.7.1)
- Create the samples and configuration databases (Section 3.7.2)
- Configure the samples and configuration databases (Section 3.7.3)
- Prepare the Internet Monitor (Section 3.7.4)
- Install the appropriate JDBC driver (Section 3.7.5)
- Modify the Internet Monitor properties file (Section 3.7.6)
- Start the Internet Monitor and verify proper functionality (Section 3.7.7)
- Implement samples database archiving if desired (Section 3.7.8)

The following sections provide more detail on each of these tasks. Throughout these sections, the Oracle 8i Enterprise Edition database is used as an example.

3.7.1 Install and Configure the Database Product

Install the alternate database product according to the manufacturer's instructions. The database can be installed either on the Internet Monitor host or on a different host. Make sure that the database is configured to be network accessible and that connections from the Internet Monitor host are allowed.

3.7.2 Create the Samples and Configuration Databases

Create two new databases, called `dcs` and `dcscfg`, using the steps appropriate for the database product. For example, the Oracle 8i Enterprise Edition database would require the following steps:

1. Run the Database Configuration Assistant.
2. Create a Typical database. Use `dcs.your_hostname` as the Global Database Name and `dcs` as the System Identifier (SID).
3. Repeat the same steps to create the `dcscfg` database, substituting `dcscfg` for `dcs` when prompted for the Global Database Name and SID.

3.7.3 Configure the Samples and Configuration Databases

For each of the two databases (`dcs` and `dcscfg`), perform the following steps:

1. Create any database product-specific constructs (such as Oracle tablespaces) associated with the creation of database users.
2. Create a user account named `dcs` within the database, identified by a password of your choice.
3. If required by the database product, grant the `dcs` user the privileges necessary for connecting to the database, reading from the database, creating new tables, and altering and writing to existing tables.

The following example illustrates how to do these steps using the Oracle 8i Enterprise Edition database:

1. Run the Oracle SQLPlus program.
2. When prompted, enter the system manager user name and password (`system` and `manager` by default), and enter `dcs` as the Host String.
3. Create a tablespace that will be used by the database. The following parameters are suggestions only; experienced Oracle administrators will probably want to adjust these values:

```
SQL> create tablespace imon_1
 2 datafile 'imon_1.dat' size 20M
 3 default storage (initial 10K next 50K minextents 1 maxextents 999)
 4 online;
```

4. Create a `dcs` user account for the database, identified by the password `dcs`. The password can be set to a different value if desired:

```
SQL> create user dcs
 2 identified by dcs
 3 default tablespace imon_1;
```

5. Grant the necessary privileges to the `dcs` user:

```
SQL> grant create session to dcs;
SQL> grant alter database to dcs;
SQL> grant create any table to dcs;
SQL> grant unlimited tablespace to dcs;
```

Next, a parallel set of steps must be repeated for the `dcscfg` database:

1. Run the Oracle SQLPlus program.
2. When prompted, enter the system manager user name and password (`system` and `manager` by default), and enter `dcscfg` as the Host String.
3. Create a tablespace that will be used by the database. The following parameters are suggestions only; experienced Oracle administrators will probably want to adjust these values:

```
SQL> create tablespace imon_2
 2 datafile 'imon_2.dat' size 20M
 3 default storage (initial 10K next 50K minextents 1 maxextents 999)
 4 online;
```

4. Create a `dcs` user account for the database, identified by the password `dcs`. The password can be set to a different value if desired:

```
SQL> create user dcs
 2 identified by dcs
 3 default tablespace imon_2;
```

5. Grant the necessary privileges to the `dcs` user:

```
SQL> grant create session to dcs;
SQL> grant alter database to dcs;
SQL> grant create any table to dcs;
SQL> grant unlimited tablespace to dcs;
```

3.7.4 Prepare the Internet Monitor

Install the Internet Monitor normally, then shut it down. If the PostgreSQL database will not be used for anything else, it can be shut down also. Use the following commands:

```
# /sbin/init.d/nsim stop

# /sbin/init.d/postgres stop
```

3.7.5 Install the Appropriate JDBC Driver

The Internet Monitor requires the appropriate JDBC driver to communicate with a database product. This driver is typically a thin Type 4 driver supplied by the database manufacturer in the form of a .jar file or .zip file. For example, the Oracle 8i Enterprise Edition database supplies a JDBC Thin Driver named `classes12.zip` which can be found in the directory `ORACLE_INSTALLDIR\ora81\jdbc\lib` on a typical Oracle on Windows installation. Consult the database product documentation to locate the JDBC driver file.

After the driver file has been located, perform the following steps:

1. On the host where the Internet Monitor is installed, copy the driver file into the `/usr/internet/monitor/web/WEB-INF/lib` directory.

If the file has a .zip extension instead of a .jar extension, rename it to give it a .jar extension. For instance, rename the Oracle 8i JDBC driver like this:

```
# mv classes12.zip classes12.jar
```

If desired the driver file name can be changed to be less generic, such as `ora81_classes12.jar` in the previous example.

2. Set the proper permissions on the driver jar file if necessary. In the Oracle 8i example, use a command like the following:

```
# chmod 644 classes12.jar
```

3.7.6 Modify the Internet Monitor Properties File

The `/usr/internet/monitor/.properties` file must be modified to define information about the selected JDBC driver, the URLs and authentication information needed to access the database, and the datatype definitions to use when creating table columns in the database. If this file does not exist, create it. Otherwise, modify the existing version.

Because the database password is stored in the `.properties` file, this file should be protected from unauthorized access by setting the file ownership and permissions appropriately, using the following commands:

```
# chown root:nsim /usr/internet/monitor/.properties
# chmod 640 /usr/internet/monitor/.properties
```

Table 3–2 details the properties that can be specified in the Internet Monitor properties file.

Table 3–2: Contents of Internet Monitor Properties File

Property Name	Description
<code>jdbc.drivers</code>	The fully specified class name of the JDBC driver.
<code>com.compaq.osis.ism.samplesDbUrl</code>	The URL that should be used to connect to the <code>dcs</code> samples database. This URL will generally contain information about the <code>host.name</code> , <code>port</code> , and <code>database</code> to connect to. See the JDBC driver documentation for the appropriate database to get exact formatting details.
<code>com.compaq.osis.ism.samplesDbUserName</code>	The user name that should be used to connect to the <code>dcs</code> samples database. This user account should have been created during the database configuration process detailed in Section 3.7.3; the recommended value was <code>dcs</code> .

Table 3–2: Contents of Internet Monitor Properties File (cont.)

Property Name	Description
<code>com.compaq.osis.ism.samplesDbPassword</code>	The password that should be used to connect to the <code>dcs</code> samples database. This password should have been set during the database configuration process detailed in Section 3.7.3.
<code>com.compaq.osis.ism.configDbUrl</code>	The URL that should be used to connect to the <code>dcscfg</code> configuration database. This URL generally contains information about the host name, port, and database to connect to. See the JDBC driver documentation for the appropriate database to get exact formatting details.
<code>com.compaq.osis.ism.configDbUserName</code>	The user name that should be used to connect to the <code>dcscfg</code> configuration database. This user account should have been created during the database configuration process detailed in Section 3.7.3. The recommended value was <code>dcs</code> .
<code>com.compaq.osis.ism.configDbPassword</code>	The password that should be used to connect to the <code>dcscfg</code> configuration database. This password should have been set during the database configuration process detailed in Section 3.7.3.
<code>com.compaq.osis.ism.DBLONG</code>	The data type used to create database columns that will hold a Java long value.
<code>com.compaq.osis.ism.DBINT</code>	The data type used to create database columns that will hold a Java integer value.
<code>com.compaq.osis.ism.DBBOOL</code>	The data type used to create database columns that will hold a one-character text string used to store Boolean values.
<code>com.compaq.osis.ism.DBTEXT</code>	The data type used to create database columns that will hold a Java text value.
<code>com.compaq.osis.ism.DBTEXTNOTNULL</code>	The data type used to create database columns that will hold a Java text value that should never be null. If not set, this property defaults to the value of <code>com.compaq.osis.ism.DBTEXT</code> with the <code>NOT NULL</code> string appended to it.
<code>com.compaq.osis.ism.DBDATE</code>	The data type used to create database columns that will hold a Java SQL date value.
<code>com.compaq.osis.ism.DBTIME</code>	The data type used to create database columns that will hold a Java SQL time value.

Some of the properties outlined in Table 3–2 specify data type strings that will be used by the Internet Monitor during SQL table creation. As an aid to choosing the proper datatypes for other databases, Table 3–3 lists the default values that are used for the PostgreSQL database and related values that are known to work for the Oracle 8i Enterprise Edition database.

Table 3–3: Default Values for PostgreSQL and Oracle 8i Databases

Data Type	PostgreSQL Data Type	Oracle 8i Data Type
com.compaq.osis.ism.DBLONG	int8	NUMERIC(20)
com.compaq.osis.ism.DBINT	int4	NUMERIC(11)
com.compaq.osis.ism.DBBOOL	BOOL	CHAR(1)
com.compaq.osis.ism.DBTEXT	TEXT	VARCHAR(254)
com.compaq.osis.ism.DBTEXTNOT-NULL	TEXT NOT NULL	VARCHAR(254) NOT NULL
com.compaq.osis.ism.DBDATE	Date	DATE
com.compaq.osis.ism.DBTIME	Date	DATE

Example 3–1 shows the lines that would be added to the `.properties` file when you are using the Oracle 8i Enterprise Edition database.

- For the `configDbUrl` and `samplesDbUrl` property settings, substitute the hostname of the machine where the database is running for `dbhost`.
- If the database and Internet Monitor are installed on the same machine, substitute `localhost` for `dbhost`.
- Port 1521 is the default Oracle listener port, but if the Oracle deployment uses a different port number, substitute that.
- If passwords other than `dcs` were chosen when creating the `dcs` user accounts for the two databases, substitute those passwords in the appropriate places.

Example 3–1: Lines Added to the Properties File for Oracle 8i Enterprise Edition Database

```

jdbc.drivers=oracle.jdbc.driver.OracleDriver
com.compaq.osis.ism.samplesDbUrl=jdbc:oracle:thin:@dbhost:1521:dcs
com.compaq.osis.ism.samplesDbUserName=dcs
com.compaq.osis.ism.samplesDbPassword=dcs
com.compaq.osis.ism.configDbUrl=jdbc:oracle:thin:@dbhost:1521:dcscfg
com.compaq.osis.ism.configDbUserName=dcs
com.compaq.osis.ism.configDbPassword=dcs
com.compaq.osis.ism.DBLONG=NUMERIC(20)
com.compaq.osis.ism.DBINT=NUMERIC(11)
com.compaq.osis.ism.DBBOOL=CHAR(1)
com.compaq.osis.ism.DBTEXT=VARCHAR(254)
com.compaq.osis.ism.DBDATE=DATE
com.compaq.osis.ism.DBTIME=DATE

```

3.7.7 Start the Internet Monitor and Verify Proper Functionality

To start the Internet Monitor and verify proper functionality:

1. Run the following command:

```
# /sbin/init.d/nsim start
```

If everything has been done correctly, the Internet Monitor should start up without errors.

2. Check the `/usr/internet/monitor/logs/dcs.log` to verify that the Internet Monitor server started and bound itself to the proper port. Also connect to the Internet Monitor administration `usre` interface on port 8086.

3. Ensure that configuration and reporting options are working correctly. After making some changes, restart the Internet Monitor to ensure that the changes are being read in from the database properly.
4. Add a sampler to a sampling host and make sure that samples reported by the sampling host are being stored correctly in the database. This can be verified either through the report UI or by connecting to the `dcs` database through an SQL command line utility and examining the contents of the `samples` table to ensure that new samples are being added properly. Be sure to connect to the database as the user `dcs` if the second method is used.

3.7.8 Implement Samples Database Archiving

The Internet Monitor database archiving feature is not supported with databases other than PostgreSQL. If this is a concern, see your database documentation for information on how to periodically archive old database records to keep the samples database from growing too large over time.

3.8 Using the Java Message Service

The Internet Monitor uses the Java Message Service (JMS) to send events to third-party Java client applications whenever samples are received or thresholds are triggered. These clients can then perform any customized filtering, response, and logging actions the programmer desires. JMS is an API in the Java 2 Platform, Enterprise Edition (J2EE). JMS provides a loosely coupled, reliable, asynchronous exchange of data and events between applications. Clients do not need to be integrated into the Internet Monitor or have any knowledge of the internals of the Internet Monitor to receive the events.

When a sample is received from an agent, the Internet Monitor publishes a `SampleReceived` message to the `monitor.samples` topic. If a new threshold has been triggered, a `ThresholdChanged` message is also published to the topic. Applications that subscribe to this topic will receive the messages. Information about the messages and their contents is detailed in the following sections

3.8.1 Contents of the SampleReceived Message

The `SampleReceived` message is posted for every sample that is received from data collection agents. The `SampleReceived` message is delivered as a `javax.jms.MapMessage`. Table 3–4 describes the message properties.

Table 3–4: SampleReceived Message Properties

Name	Type	Description
<code>AgentName</code>	<code>String</code>	Host name of the system running the agent
<code>SamplerId</code>	<code>String</code>	Sampler ID (name)
<code>MessageType</code>	<code>String</code>	The string <i>SampleReceived</i>

The agent name, sampler ID, and message type are sent as message properties. This allows a client to use the JMS message selection mechanism to filter the messages it receives based on these values. The message properties are accessed using the `javax.jms.MapMessage.getStringProperty()` method. For example:

```
javax.jms.MapMessage msg;
String property = msg.getStringProperty("AgentName");
```

3.8.2 Properties of the SampleReceived Message Body

Table 3–5 lists the properties of the SampleReceived message body. Values marked as optional cannot be in the message.

Table 3–5: SampleReceived Message Body Properties

Name	Type	Optional	Description
SamplerType	String		One of the standard sampler types (HTTP, LDAP, IMAP, POP, SMTP, FTP, NNTP, DNS, RADIUS, CONNECTION) or a user defined type.
SamplerHost	String		Host name of the system running the service.
SamplerPort	int		Port number of the service.
SamplerPollInterval	int		The number of milliseconds to wait between sampling.
SamplerDescription	String	*	Description field of the sampler.
TimeStamp	long		Time the sample was received. This is the difference, measured in milliseconds, between the current time and midnight, January 1, 1970 UTC. This can be used with <code>java.util.Date(long)</code> to extract the date information.
ResponseTime	long		Sample response time in milliseconds.
ByteCount	long		Number of bytes returned by the server.
ServerMessage	String		Message returned by the server.
ServerStatus	int		Status value returned by the server.
ServerInaccessible	Boolean		Indicates the server was inaccessible.
ServerError	Boolean		Indicates there was an error when connecting to the server.
ThresholdId	String		Threshold ID (name). The threshold described by this field and the following threshold fields is the threshold that is applicable to this individual sample. It does not indicate the last threshold that was triggered as a result of a sufficient number of consecutive samples exceeding the threshold.
ThresholdValue	long		Response time to trigger this threshold: value \geq 0 is a response time. -1 is server error. -2 is server inaccessible.
ThresholdLabel	String	*	Threshold label specified by the user.
ThresholdColor	String	*	Threshold color specified by the user.
ThresholdTrigger	String		Number of consecutive samples needed to trigger this threshold.
ThresholdAction	String		Action type: <i>none</i> , <i>email</i> , or <i>system_call</i> .
ThresholdEmailAddress	String	*	E-mail address to which the alert message is sent when the action type is <i>email</i> .

Table 3–5: SampleReceived Message Body Properties (cont.)

Name	Type	Optional	Description
ThresholdEmailSubject	String	*	E-mail subject of the alert message when the action type is <i>email</i> .
ThresholdSystemCall	String	*	System call made for the alert when the action type is <i>system_call</i> .

The message content values are accessed using the get methods of `javax.jms.MapMessage`. For example:

```
javax.jms.MapMessage msg;
String host = msg.getString("SamplerHost");
int port = msg.getInt("SamplerPort");
```

3.8.3 Contents of the ThresholdChanged Message

The `ThresholdChanged` message is posted whenever a threshold action is triggered. The message contains information about both the threshold that was triggered and the previously triggered threshold. This allows clients that perform functions such as setting and clearing alarm conditions to react appropriately. The `ThresholdChanged` message is delivered as a `javax.jms.MapMessage`. Table 3–6 describes the message properties.

Table 3–6: ThresholdChanged Message Properties

Name	Type	Description
AgentName	String	Host name of the system running the agent
SamplerId	String	Sampler ID (name)
MessageType	String	The string <i>ThresholdChanged</i>

3.8.4 Properties of the ThresholdChanged Message Body

Table 3–7 lists the contents of the `ThresholdChanged` message body. Values marked as optional may not be included in the message.

Table 3–7: ThresholdChanged Message Body Properties

Name	Type	Optional	Description
SamplerType	String		One of the standard sampler types (HTTP, LDAP, IMAP, POP, SMTP, FTP, NNTP, DNS, RADIUS, CONNECTION) or a user defined type.
SamplerHost	String		Host name of the system running the service.
SamplerPort	int		Port number of the service.
SamplerPollInterval	int		Number of milliseconds to wait between sampling.
SamplerDescription	String	*	Description field of the sampler.
TimeStamp	long		Time the sample was received. This is the difference, measured in milliseconds, between the current time and midnight, January 1, 1970 UTC. This can be used with <code>java.util.Date(long)</code> to extract the date information.
ResponseTime	long		Sample response time in milliseconds.

Table 3–7: ThresholdChanged Message Body Properties (cont.)

Name	Type	Optional	Description
ByteCount	long		Number of bytes returned by the server.
ServerMessage	String		Message returned by the server.
ServerStatus	int		Status value returned by the server.
ServerInaccessible	Boolean		Indicates the server was inaccessible.
ServerError	Boolean		Indicates there was an error when connecting to the server.
NewThresholdId	String		Threshold ID (name) of the triggered threshold. If the response time moved into a range where no threshold was applicable, this value is set to "No threshold" and none of the other <code>NewThresholdxxxsettings</code> are included in the message.
NewThresholdValue	long		Response time to trigger the threshold: value ≥ 0 is a response time. –1 is server error. –2 is server inaccessible.
NewThresholdLabel	String	*	Threshold label specified by the user.
NewThresholdColor	String	*	Threshold color specified by the user.
NewThresholdTrigger	int		Number of consecutive samples needed to trigger this threshold.
NewThresholdAction	String		Action type: <i>none</i> , <i>email</i> , or <i>system_call</i> .
NewThresholdEmailAddress	String	*	E-mail address to which the alert message is sent when the action type is <i>email</i> .
NewThresholdEmailSubject	String	*	E-mail subject of the alert message when the action type is <i>email</i> .
NewThresholdSystemCall	String	*	System call made for the alert when the action type is <i>system_call</i> .
OldThresholdId	String		Threshold ID (name) of the last threshold that was triggered prior to the current triggering event. If the response time moved out of a range where no threshold was applicable, this value is set to "No threshold" and none of the other <code>OldThresholdxxxsettings</code> are included in the message.
OldThresholdValue	long		Response time to trigger the threshold: value ≥ 0 is a response time. –1 is server error. –2 is server inaccessible.
OldThesholdLabel	String	*	Threshold label specified by the user.
OldThresholdColor	String	*	Threshold color specified by the user.
OldThresholdTrigger	int		Number of consecutive samples needed to trigger this threshold.
OldThresholdAction	String		Action type: <i>none</i> , <i>email</i> , or <i>system_call</i> .

Table 3–7: ThresholdChanged Message Body Properties (cont.)

Name	Type	Optional	Description
NewThresholdEmailAddress	String	*	E-mail address to which the alert message is sent when the action type is <i>email</i> .
OldThresholdEmailSubject	String	*	E-mail subject of the alert message when the action type is <i>email</i> .
OldThresholdSystemCall	String	*	System call made for the alert when the action type is <i>system_call</i> .

3.8.5 Accessing the JMS Class Files

The Internet Monitor provides the JMS class files in the `/usr/internet/monitor/jms/jars` directory. Most applications will require the `smqclient.jar`, `jms.jar`, and `jndi.jar` files.

3.8.6 Running the Sample JMS Client Application

A sample JMS client application is included with the Internet Monitor. To run the sample client application, change directory to the `/usr/internet/monitor/web/examples/jms` and run the `monitorclient` script. The application will connect to the Internet Monitor JMS server and subscribe to the `monitor.samples` topic. When the Internet Monitor server receives a sample from one of the agents, a message is sent to all JMS clients that have subscribed to the topic. The sample JMS client application prints the contents of the message.

3.8.7 Specifying the JMS Configuration

JMS client applications must call the `context.close()` method on the context that was returned by the `InitialContext()` call. This releases resources on the JMS server. An example of this can be seen in the sample JMS client (Section 3.8.6).

A good practice is to use properties to specify the JMS configuration for an application. This allows the application to work with different JMS servers without changes to the application code. To do this, use the no argument Java Naming and Directory Interface (JNDI) `InitialContext()` method and specify the JNDI properties in a `jndi.properties` file or on the command line.

The Internet Monitor uses SwiftMQ for the JMS server. (See <http://www.swiftmq.com>.) SwiftMQ requires a client application to set the following JNDI properties:

```
java.naming.factory.initial=com.swiftmq.jndi.InitialContextFactoryImpl
java.naming.provider.url=smqp://hostname:4001/timeout=10000
```

- The properties can be set on the command line using the `-D` option as follows:

```
> java \
  -Djava.naming.factory.initial=com.swiftmq.jndi.InitialContextFactoryImpl \
  -Djava.naming.provider.url=smqp://hostname:4001/timeout=10000
```

- The properties can be set in a file named `jndi.properties`. Create a file named `jndi.properties` that contains the following two lines:

```
java.naming.factory.initial=com.swiftmq.jndi.InitialContextFactoryImpl
java.naming.provider.url=smqp://hostname:4001/timeout=10000
```

Place the `jndi.properties` file in a directory that is in the application classpath. The Java runtime will read all files named `jndi.properties` that are located in the classpath and add the properties to the application.

For either option, replace *hostname* in the second property with the name of the system running the Internet Monitor. The `timeout=10000` part of the URL specifies the maximum number of milliseconds to wait for the JNDI lookup.

3.9 Using the Performance Monitor Applet in a Cluster Environment

When running the Internet Monitor in a cluster, additional configuration is required to run the Performance Monitor applet.

By default, the Java security manager allows a Java applet to accept socket connections from the host that the Web browser is connected to when running the applet. Socket connections from any other host are not allowed. This presents a problem when the Internet Monitor is running on a cluster. To run the Performance Monitor applet the Web browser connects to the Internet Monitor using the cluster alias. Since socket connections are from the individual hosts in the cluster, not the cluster alias, the Performance Monitor applet will not accept the connection.

To allow the Performance Monitor applet to accept socket connections from the cluster members, a `SocketPermission` entry must be added to the user policy file for each cluster member. For example, assume the Internet Monitor is running on a three-node cluster with host names `host1.your.domain`, `host2.your.domain`, `host3.your.domain` and the cluster alias `alias.your.domain`. Add the following entry to the user policy file:

```
grant codeBase "http://alias.your.domain:8086/class/monitor.jar" {
  permission java.net.SocketPermission "host1.your.domain:1024-", "accept, resolve";
  permission java.net.SocketPermission "host2.your.domain:1024-", "accept, resolve";
  permission java.net.SocketPermission "host3.your.domain:1024-", "accept, resolve";
};
```

The location of the user policy file is as follows:

`user.home/.java.policy` (Tru64 UNIX)

`user.home\.java.policy` (Windows)

where `user.home` is the user's home directory. On Tru64 UNIX this is the user's home directory, such as `/home/user`. On Windows, given the user name `userName`, `user.home` defaults to:

<code>C:\Documents and Settings\userName</code>	(Windows 2000 and Windows XP)
<code>C:\Winnt\Profiles\userName</code>	(multi-user Windows NT)
<code>C:\Windows\Profiles\userName</code>	(multi-user Windows 95)
<code>C:\Windows</code>	(single-user Windows 95)

Additional information on Java policy files may be found at <http://java.sun.com/products/jdk/1.2/docs/guide/security/index.html>.

Administering the Internet Monitor

The Internet Monitor enables you to see how your Internet services are performing.

4.1 Starting and Stopping the Internet Monitor

To enable or disable the Internet Monitor, you use the Start/Stop the Internet Monitor menu option from the Administration utility for Internet Express, as follows:

1. From the Administration utility for Internet Express, choose Manage Components.
2. On the Manage Components menu, choose Start/Stop the Internet Monitor. The resulting page identifies whether the Internet Monitor is currently running.
 - To start the Internet Monitor, click on Restart.
 - To stop the Internet Monitor, click on Stop.

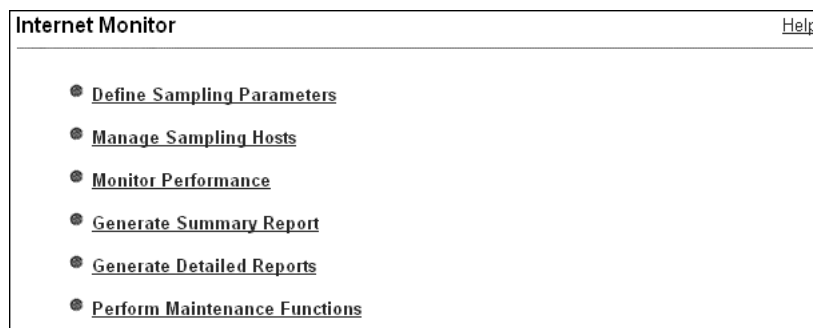
4.2 Accessing the Internet Monitor

You can access the Internet Monitor application in the following ways:

- Using the Administration utility for Internet Express. To use this option, choose Internet Monitor under Quality of Service on the Manage Components menu.
- Using a Web browser, without going through the Administration utility for Internet Express. The Internet Express installation installs the Internet Monitor administration server on port 8086.

After you access the Internet Monitor URL, the Internet Monitor main menu (Figure 4–1) is displayed.

Figure 4–1: Internet Monitor Main Menu



From the Internet Monitor menu, you can choose the following options:

- Define sampling parameters (Section 4.3)
- Manage sampling hosts (Section 4.4)
- Monitor performance (Section 4.5)
- Generate summary report (Section 4.6)
- Generate detailed reports (Section 4.7)

- Perform maintenance functions (Section 4.8)

4.3 Defining Sampling Parameters

When you choose Define Sampling Parameters from the Internet Monitor main menu, the Define Sampling Parameters menu is displayed.

A sampler is an object that defines a set of sampling operations that an agent performs while measuring the total elapsed time it takes for the set of operations to complete.

To create, modify, or delete samplers, choose the initial Define Sampling Parameters menu (Figure 4–2), and then fill out succeeding menus.

Figure 4–2: Define Sampling Parameters Menu

The screenshot shows the 'Define Sampling Parameters' menu. At the top, there is a 'Home' link and a 'Help' link. The main title is 'Define Sampling Parameters'. Below this, there is a section titled 'Create a New Sampler'. In this section, there is a 'Select Sampler:' dropdown menu with 'HTTP' selected, and a 'Create' button. Below the dropdown menu, there is a 'Modify' button. The main area of the menu is divided into sections for different protocols: IMAP, FTP, CONNECTION, LDAP, DNS, SMTP, NNTP, POP3, and RADIUS. Each section contains one or more entries, each with a 'Modify sampler | thresholds' button and a 'Remove' button. The entries are: IMAP on imaphub, FTP on dylan.abc, Connection on dylan, LDAP on travel.xyzcorp.com, DNS on dylan.abc.wilbry.com, SMTP on dylan.abc.wilbry.com, NNTP on petty.abc.wilbry.com, POP on imaphub.xyzcorp.com, and RADIUS on dylan.abc.wilbry.com.

If no samplers currently exist, the Define Sampling Parameters menu shows only the Create a New Sampler option. If samplers have been previously defined, the Define Sampling Parameters menu also shows a Modify Sampler, Modify Thresholds, and Remove Sampler section.

From the Define Sampling Parameters menu, you have the following options:

- Create, modify, or remove HTTP samplers and Modify Thresholds (Section 4.3.1)
- Create, modify, or remove NNTP samplers and Modify Thresholds (Section 4.3.2)
- Create, modify, or remove POP samplers and Modify Thresholds (Section 4.3.3)
- Create, modify, or remove IMAP samplers and Modify Thresholds (Section 4.3.4)

- Create, modify, or remove SMTP samplers and Modify Thresholds (Section 4.3.5)
- Create, modify, or remove FTP samplers and Modify Thresholds (Section 4.3.6)
- Create, modify, or remove LDAP samplers and Modify Thresholds (Section 4.3.7)
- Create, modify, or remove DNS samplers and Modify Thresholds (Section 4.3.8)
- Create, modify, or remove RADIUS samplers and Modify Thresholds ()
- Create, modify, or remove Connection samplers and Modify Thresholds ()

Section 3.3 provides guidelines on how to deploy samplers.

All sampler menus include a Port field. You use this field to indicate the port number of the server. Table 4–1 shows the default port numbers assigned for each service. You can either accept these default port numbers, or change them.

Table 4–1: Default Port Numbers

Service	Default Port Number
HTTP	80
NNTP	119
POP	110
IMAP	143
SMTP	25
FTP	21
LDAP	389
DNS	53
RADIUS	1812
Connection	None

4.3.1 Managing HTTP Samplers

The Internet Monitor allows you to monitor the response time of servers that implement the HyperText Transfer Protocol (HTTP). HTTP samplers measure the amount of time that a Web server or proxy server takes to serve documents.

When creating or modifying HTTP samplers, you supply a list of Uniform Resource Identifiers (URIs) to be accessed by the Web browser for sampling. For example, if the complete URL is `http://www.mycompany.com/index.html`, the URI portion is `index.html`.

A URI can optionally have a query string appended to it, allowing you to measure the performance of the Web server when executing Common Gateway Interface (CGI) scripts that require parameters to be passed to them.

From the Define Sampling Parameters menu, the following options are available:

- Create HTTP Samplers (Section 4.3.1.1)
- Modify or Remove HTTP Samplers (Section 4.3.1.2)

Table 4–2 describes the HTTP Sampler menu fields.

Table 4–2: HTTP Sampler Menu Fields

Field	Description
Description	A text string that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Host name of the server that is being polled by the sampler.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
Connection Type	Type of connection to be used for the sampler. Choose either HTTP or Secure (SSL). The default value is HTTP.
Proxy Server	Specifies whether a proxy server should be used for the sampler. This section includes a checkbox to indicate Use Proxy Server, and a Host field for specifying the name of the Proxy Server.
User Name	If the specified URIs require authentication, this field specifies an authorized user name.
Password	The password for an authorized user.
Documents to Retrieve	In this section, enter the pathname for the URI to be accessed by the HTTP sampler. By default, the pathname is <code>index.html</code> . Use the option button to select the HTTP method to be performed: either GET or POST.
Allow cached documents	Controls whether the server can return a cached version of the document.
Use Proxy Server	Specifies that a proxy server is to be used when connecting to the HTTP server.
Proxy Host	Host name or IP address of the proxy server.
Proxy Port	Port number of the proxy server.

4.3.1.1 Creating an HTTP Sampler

To create an HTTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select HTTP.
3. Click on Create.
The Create HTTP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is HTTP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: `HTTP on server.host.name`.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, select the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the host (Web server or proxy server) to be polled by the agent.

8. In the Port field, either accept the default number of the server's port (Table 4-1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. In the Connection Type section, select either HTTP (default) or Secure (SSL).
11. If you want to use a proxy server, select the Use Proxy Server checkbox, and enter the name of the proxy server in the Host field next to the Use Proxy Server box.
12. When you create an HTTP sampler, you create a list of multiple HTTP operations to be associated with the sampler. This list must contain at least one document and pathname.
 - a. Use the option button to choose either GET or POST as the HTTP method to be polled.
 - b. In the Documents to Retrieve section, enter the pathname for the URI to be accessed in the input field.
 - c. Click on Add to add it to the list. To add more pathnames to be accessed, repeat this step.
 - d. To remove an item from the list, select the item from the Documents to Retrieve list and click on Remove. To delete more pathnames from the list, repeat this step.
13. If desired, click in the box next to Allow cached documents.
14. If the specified URIs require authentication, enter an authorized user name in the User Name field, enter a password for an authorized user in the Password field.
15. If you want to use a proxy server for the HTTP sampler, complete the Proxy Server portion of the menu:
 - a. Click in the box next to Use Proxy Server.
 - b. Enter a host name or IP address in the Host field.
 - c. Enter a port number for the proxy host in the Port field.
16. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.

Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
17. Click on Create.
18. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.

The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.

The Modify Threshold menu is displayed. For a description of the fields, see Table 4-12.

- To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.1.2 Modifying or Removing an HTTP Sampler

To modify or remove an HTTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.
A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.
The Modify HTTP Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–2 describes the HTTP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.
The Define Thresholds menu is displayed.
4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.
The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.2 Managing NNTP Samplers

The Internet Monitor allows you to monitor the performance of news servers that implement the Network News Transfer Protocol (NNTP). An NNTP sampler downloads headers and articles from newsgroups.

From the Define Sampling Parameters menu, the following options are available:

- Create NNTP Samplers (Section 4.3.2.1)
- Modify or Remove NNTP Samplers (Section 4.3.2.2)

Table 4–3 describes the NNTP Sampler menu fields.

Table 4–3: NNTP Sampler Menu Fields

Field	Description
Description	A text string that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Host name of the server that is being polled by the sampler.
Port	Port number of the server.

Table 4–3: NNTP Sampler Menu Fields (cont.)

Field	Description
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
Newsgroup Name	Name of the newsgroup to be accessed.

4.3.2.1 Creating an NNTP Sampler

To create an NNTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select NNTP.
3. Click on Create.
The Create NNTP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is NNTP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: NNTP on *server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, select the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the news host to be polled.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. When you create an NNTP sampler, you build a list of multiple newsgroups to be polled. This list must contain at least one newsgroup.
 - a. In the Newsgroups to Retrieve section, enter the name of the newsgroup to be accessed in the input field. Click on Add to add it to the list. To add more newsgroups to be accessed, repeat this step.
 - b. To remove an item from the list, select the item from the Newsgroups list and click on Remove. To remove more newsgroups, repeat this step.
11. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
12. Click on Create.

13. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.
The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.
 - To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.2.2 Modifying or Removing an NNTP Sampler

To modify or remove an NNTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.
A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.
The Modify NNTP Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–3 describes the NNTP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.
The Define Thresholds menu is displayed.
4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.
The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.3 Managing POP Samplers

The Internet Monitor allows you to monitor the message download response time of mail servers that implement the Post Office Protocol (POP).

When you create and modify samplers for POP, you specify the user name and password of a user whose POP mailbox is to be accessed. Typically, this is not an actual end user, but a test user, for whom a POP E-mail account and several messages have been created. The POP sampler downloads messages from the user's inbox and does not delete them from the POP server after downloading.

From the Define Sampling Parameters menu, the following options are available:

- Create POP Samplers (Section 4.3.3.1)

- Modify or Remove POP samplers (Section 4.3.3.2)

Table 4–4 describes the POP Sampler menu fields.

Table 4–4: POP Sampler Menu Fields

Field	Description
Description	A text string that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Host name of the server that is being polled by the sampler.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
User Name	Name of user whose mailbox is to be sampled.
Password	Password for the user.
Number of Messages	Number of messages to be downloaded.

4.3.3.1 Creating a POP Sampler

To create a POP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select POP.
3. Click on Create.
The Create POP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is POP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: POP on *server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, select the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the POP mail server host to be polled.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. In the User Name field, enter the user name of the user whose mailbox is to be sampled.
11. In the Password field, enter the password of the user.

12. In the Number of Messages field, enter the number of messages to be downloaded. You should ensure that the specified number of messages actually exists in the user's INBOX.
13. When you create a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
14. Click on Create.
15. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.
The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.
 - To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.3.2 Modifying or Removing a POP Sampler

To modify or remove a POP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.
A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.
The Modify POP Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–4 describes the POP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.
The Define Thresholds menu is displayed.
4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.
The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.4 Managing IMAP Samplers

The Internet Monitor allows you to monitor the message download response time of mail servers that implement the Interactive Mail Access Protocol (IMAP).

When you create and modify samplers for IMAP, you specify the user name and password of a user whose IMAP mailbox is to be accessed. Typically, this is not an actual end user, but a test user for whom an IMAP E-mail account and several messages have been created. The IMAP sampler downloads messages from the user's inbox and does not delete them from the IMAP server after downloading.

From the Define Sampling Parameters menu, the following options are available:

- Create IMAP Samplers (Section 4.3.4.1)
- Modify or Remove IMAP Samplers (Section 4.3.4.2)

Table 4–5 describes the IMAP Sampler menu fields.

Table 4–5: IMAP Sampler Menu Fields

Field	Description
Description	A text string that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Host name of the server that is being polled by the sampler.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
User Name	Name of user whose mailbox is to be sampled.
Password	Password for the user.
Number of Messages	Number of messages to be downloaded.

4.3.4.1 Creating an IMAP Sampler

To create an IMAP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select IMAP.
3. Click on Create.
The Create IMAP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is IMAP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: *IMAP on server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, select the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the IMAP mail server host to be polled.

8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. In the User Name field, enter the user name of the user whose mailbox is to be sampled.
11. In the Password field, enter the password of the user.
12. In the Number of Messages field, enter the number of messages to be downloaded.
13. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host. Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
14. Click on Create.
15. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds. The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold. The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.
 - To create a new threshold, click on Create. The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.4.2 Modifying or Removing an IMAP Sampler

To modify or remove an IMAP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu. The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler. A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler. The Modify IMAP Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–5 describes the IMAP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.

The Define Thresholds menu is displayed.

4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.

The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.

5. To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.5 Managing SMTP Samplers

The Internet Monitor allows you to monitor the response time of servers that implement the Simple Mail Transfer Protocol (SMTP). The SMTP sampler sends a test message to the specified SMTP server and measures the response time. Typically, you would set up a test mail account to receive the E-mail messages sent by the SMTP sampler and delete them automatically upon receipt.

From the Define Sampling Parameters menu, the following options are available:

- Create SMTP Samplers (Section 4.3.5.1)
- Modify or Remove SMTP Samplers (Section 4.3.5.2)

Table 4–6 describes the SMTP Sampler menu fields.

Table 4–6: SMTP Sampler Menu Fields

Field	Description
Description	A text field that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Host name of the server that is being polled by the sampler.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
Address Recipient	E-mail address to which the test E-mail messages will be sent by the SMTP server.
Message URL	Uniform Resource Locator (URL) for a file containing text that will comprise the body of the test mail message. If no URL is specified, a default message body will be used. The default message body is: Internet Monitor test message The sender is: Internet Monitor <nsim@hostname>

4.3.5.1 Creating an SMTP Sampler

To create an SMTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select SMTP.
3. Click on Create.
The Create SMTP Sampler menu is displayed.

4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is SMTP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: *SMTP on server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, choose the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the SMTP server host to be polled.
8. In the Port field, either accept the default number of the server's port (Table 4-1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the radio button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list box and choose another value.
10. In the Address Recipient field, enter the E-mail address to which the test E-mail messages will be sent by the SMTP server.
11. In the Message URL field, enter the URL for a file containing text that will comprise the body of the test mail message.
12. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
13. Click on Create.
14. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.
The Modify Threshold menu is displayed. For a description of the fields, see Table 4-12.
 - To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4-12.

4.3.5.2 Modifying or Removing an SMTP Sampler

To modify or remove an SMTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.

A confirmation message is displayed.

3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.

The Modify SMTP Samplers menu is displayed.

- Revise the values in any of the fields. Table 4–6 describes the SMTP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
- Click on Modify.

The Define Thresholds menu is displayed.

4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.

The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.

5. To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.6 Managing FTP Samplers

FTP samplers measure the amount of time that an agent takes to complete a File Transfer Protocol (FTP) operation from a specific server.

From the Define Sampling Parameters menu, the following options are available:

- Create FTP samplers (Section 4.3.6.1)
- Modify or Remove FTP samplers (Section 4.3.6.2)

Table 4–7 describes the FTP sampler menu fields.

Table 4–7: FTP Sampler Menu Fields

Field	Description
Description	A text string that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Name of the host to be accessed by the FTP sampler.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
User Name	Name of the user on the server whose files are to be accessed.
Password	Password of the user on the server whose files are to be accessed.
After Login Change Directory to:	Directory to be accessed on the server using the FTP sampler. The default is the login directory. Leave this field empty to get the default.
Select Command	An FTP command to be performed by the sampler: <code>get</code> , <code>pwd</code> , or <code>ls</code> . If you select the <code>get</code> command, type the name of a file to be accessed using the FTP sampler in the input field.

4.3.6.1 Creating an FTP Sampler

To create an FTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select FTP.
3. Click on Create.
The Create FTP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is FTP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: *FTP on server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, choose the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the server host to be accessed by the FTP operation.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. In the After Login Change Directory to: field, enter the pathname.
11. In the User Name field, enter the user name.
12. In the Password field, enter the password.
13. In the FTP Server Directory field, enter the directory to be accessed using the FTP sampler. The default if left empty is the FTP login directory.
 - a. Use the option button to choose the FTP action to be executed on the server. If you choose the *get* command, enter the name of a standard file to be accessed in the input field.
 - b. Click on Add to add it to the list. To add more commands to be executed, repeat this step.
 - c. To remove an item from the list, select the item from the FTP Server Directory and Commands list and click on Delete.
14. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
15. Click on Create.
16. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.

The Define Sampling Parameters menu is displayed.

- To modify an existing threshold, click on Modify next to the desired threshold.

The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.

- To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.6.2 Modifying or Removing an FTP Sampler

To modify or remove an FTP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.

The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).

2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.

A confirmation message is displayed.

3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.

The Modify FTP Samplers menu is displayed.

- Revise the values in any of the fields. Table 4–7 describes the FTP Sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
- Click on Modify.

The Define Thresholds menu is displayed.

4. To modify the threshold values or add new threshold values, click on Modify next to the name of the desired threshold.

The Modify Thresholds menu is displayed. For a description of the fields, see Table 4–12.

5. To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.7 Managing LDAP Samplers

Lightweight Directory Access Protocol (LDAP) samplers measure the amount of time it takes to connect to an LDAP-based directory server and perform the specified directory search.

From the Define Sampling Parameters menu, the following options are available:

- Create LDAP Samplers (Section 4.3.7.1)
- Modify or Remove LDAP Samplers (Section 4.3.7.2)

Table 4–8 describes the LDAP sampler menu fields.

Table 4–8: LDAP Sampler Menu Fields

Field	Description
Description	A text field that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Name of the host to be accessed by the LDAP operation.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
Port	Port number of the server.
Search Base	A distinguished name that indicates the directory subtree to be searched (for example, o=Compaq, c=US). This parameter is required.
Search Filter	A valid LDAP search filter (for example, cn=Joe Cool). This parameter is required.
Bind Domain Name	A distinguished name used to authenticate the search to the directory server before attempting the search. This parameter is optional. If it is not supplied, an unauthenticated search will be attempted.
Bind Password	Password for authenticating to the directory server before attempting the search. The Bind Password parameter is optional; you should set a value for this field only if you also entered a value in the Bind Domain Name field.

4.3.7.1 Creating an LDAP Sampler

To create an LDAP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select LDAP.
3. Click on Create.
The Create LDAP Sampler menu is displayed.
4. If desired, in the Description field, enter a description of the sampler.
By default, the description name is LDAP Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: LDAP on *server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, choose the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the host to be accessed by the LDAP operation.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.

10. In the Search Base field, enter the desired distinguished name.
11. In the Search Filter field, enter a valid LDAP search filter.
12. In the Bind Domain Name field, enter the distinguished name used to authenticate the search to the directory server.
13. In the Bind Password field, enter the password for authenticating the directory server.
14. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
15. Click on Create.
16. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.
The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.
 - To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.7.2 Modifying or Removing an LDAP Sampler

To modify or remove an LDAP sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.
A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.
The Modify LDAP Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–8 describes the LDAP sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.
The Define Thresholds menu is displayed.
4. To modify the threshold values or add new threshold values, click on Modify Thresholds next to the name of the desired sampler.
The Define Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.8 Managing DNS Samplers

DNS samplers measure the amount of time that an agent takes to connect to a Domain Name Service (DNS) server and perform an address lookup for each host name in a specified list.

From the Define Sampling Parameters menu, the following options are available:

- Create DNS Samplers (Section 4.3.8.1)
- Modify or Remove DNS Samplers (Section 4.3.8.2)

Table 4–9 describes the DNS sampler menu fields.

Table 4–9: DNS Sampler Menu Fields

Field	Description
Description	A text field that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Name of the host to be accessed by the DNS operation.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.

4.3.8.1 Creating a DNS Sampler

To create a DNS sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select DNS.
3. Click on Create.
The Create DNS Sampler menu is displayed.
4. In the Description field, enter a description of the sampler.
By default, the description name is DNS Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: *DNS on server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, select the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the host (Web server or proxy server) to be polled by the agent.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds

- Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. When you create a DNS sampler, you build a list of host names that the DNS server will be asked to resolve. This list must contain at least one host name.
 - a. In the Host names to look up section, enter a host name to be looked up in the input field.
 - b. Click on Add to add it to the list. To add more host names to be accessed, repeat this step.
 - c. To remove an item from the list, select the item from the Host Name list and click on Remove. To remove more hosts from the list, repeat this step.
 11. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.

Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
 12. Click on Create.
 13. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.

The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.

The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.
 - To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.8.2 Modifying or Removing a DNS Sampler

To modify or remove a DNS sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.

The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.

A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.

The Modify DNS Samplers menu is displayed.

 - Revise the values in any of the fields. Table 4–9 describes the DNS sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.

The Define Thresholds menu is displayed.

4. To modify the threshold values or add new threshold values, click on Modify Thresholds next to the name of the desired sampler.
The Define Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.9 Managing RADIUS Samplers

The Internet Monitor allows you to monitor the response time of servers that implement the Remote Authentication Dial In User Service (RADIUS) protocol. RADIUS samplers measure the amount of time required to connect to a RADIUS server and authenticate a specified user.

RADIUS servers are typically configured with a list of IP addresses from which client authentication attempts are allowed. Be sure to configure any RADIUS server being monitored to allow authentication requests from the hosts where data collection agents are running. If you fail to do so, most RADIUS servers will silently ignore the agent’s connection requests, eventually causing the agent to report that the server is inaccessible.

From the Define Sampling Parameters menu, the following options are available:

- Create RADIUS Sampler (Section 4.3.9.1)
- Modify or Remove RADIUS Samplers (Section 4.3.9.2)

Table 4–10 describes the RADIUS sampler menu fields.

Table 4–10: RADIUS Sampler Menu Fields

Field	Description
Description	A text field that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Name of the host to be accessed by the RADIUS operation.
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.
Shared Secret	A text string that the RADIUS server has been configured to expect from connecting clients.
User Name	Name of the authenticating user. The name may contain a realm (myname@xyz.com) or just the name itself (myname).
Password	Password associated with the authenticating user.
Maximum Number of Attempts	Maximum number of times to attempt the authentication if the server fails to respond. Because RADIUS uses the connectionless UDP protocol, it is possible for packets to be dropped and connection attempts to fail in some circumstances. This parameter allows multiple attempts to be made in these cases. The response time reported after an eventual success will include the accumulated time spent making the initial failed requests in addition to the time required to make the successful one.

4.3.9.1 Creating a RADIUS Sampler

To create a RADIUS sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select RADIUS.
3. Click on Create.
The Create RADIUS Sampler menu is displayed.
4. In the Description field, enter a description of the sampler.
By default, the description name is RADIUS Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: RADIUS on *server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, choose the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the host to be accessed by the RADIUS server operation.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. In the Shared secret field, enter a text string that the RADIUS server will expect to receive from connecting clients.
11. In the User Name field, enter the name of the user who will be authenticating the RADIUS connection.
12. In the Password field, enter the password associated with the authenticating user.
13. In the Maximum Number of Attempts field, enter the maximum number of times to attempt the authentication if the server fails to respond.
14. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
15. Click on Create.
16. The Define Thresholds page is displayed. By default, three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.

The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.

- To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.9.2 Modifying or Removing a RADIUS Sampler

To modify or remove a RADIUS sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.

The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).

2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.

A confirmation message is displayed.

3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.

The Modify RADIUS Samplers menu is displayed.

- Revise the values in any of the fields. Table 4–10 describes the RADIUS sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
- Click on Modify.

The Define Thresholds menu is displayed.

4. To modify the threshold values or add new threshold values, click on Modify Thresholds next to the name of the desired sampler.

The Define Thresholds menu is displayed. For a description of the fields, see Table 4–12.

5. To create a new threshold, click on Create.

The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.10 Managing Connection Samplers

Connection samplers measure the amount of time that an agent takes to connect to and then immediately disconnect from an arbitrary host and port.

From the Define Sampling Parameters menu, the following options are available:

- Create Connection Samplers (Section 4.3.10.1)
- Modify or Remove Connection Samplers (Section 4.3.10.2)

Table 4–11 describes the Connection sampler menu fields.

Table 4–11: Connection Sampler Menu Fields

Field	Description
Description	A text field that describes the sampler.
Sampling Interval	Amount of time for the sampler to wait between each poll of the server.
Server Host Name	Name of the host to be accessed by the connection operation.

Table 4–11: Connection Sampler Menu Fields (cont.)

Field	Description
Port	Port number of the server.
Connection Timeout	Maximum amount of time allowed for the sampler to connect to the server. Once the connection is established, it is the maximum amount of time a read operation is allowed to stall during sampling.

4.3.10.1 Creating a Connection Sampler

To create a Connection sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed.
2. Under Create a New Sampler, pull down the list next to Select Sampler and select CONNECTION.
3. Click on Create.
The Create Connection Sampler menu is displayed.
4. In the Description field, enter a description of the sampler.
By default, the description name is Connection Sampler. If you do not enter a name in this field, the description will be updated with the Server Host Name appended in the format: *Connection on server.host.name*.
5. In the Sampling Interval field, enter a numeral to specify the interval value.
6. In the drop-down list next to Sampling Interval, choose the unit for the interval: seconds, minutes, or hours.
7. In the Server Host Name field, enter the name of the host to be accessed by the Connection operation.
8. In the Port field, either accept the default number of the server's port (Table 4–1), or enter a new value.
9. Specify a connection timeout value. You can either:
 - Use the default timeout value of 30 seconds.
 - Choose another value by clicking on the option button, and then enter a new value in the field. To specify an interval other than seconds, pull down the list and choose another value.
10. When creating a sampler, you can attach it to a sampling host identified by a host name. A sampler can be attached to more than one sampling host.
Systems currently defined as sampling hosts are listed in the section of the menu labeled Perform Sampling from the Following Hosts. To attach the new sampler to one or more of these sampling hosts, select the check box next to the name of the desired host.
11. Click on Create.
12. The Define Thresholds page is displayed. By default three thresholds are defined: Server Inaccessible, Server Error, and Response Time > 0 ms.
 - To accept the defaults, click on Finished With Thresholds.
The Define Sampling Parameters menu is displayed.
 - To modify an existing threshold, click on Modify next to the desired threshold.
The Modify Threshold menu is displayed. For a description of the fields, see Table 4–12.

- To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.10.2 Modifying or Removing a Connection Sampler

To modify or remove a Connection sampler, follow these steps:

1. Choose Define Sampling Parameters from the Internet Monitor menu.
The Define Sampling Parameters menu is displayed. All samplers currently defined are shown in tabular format under the appropriate category (HTTP, NNTP, POP, IMAP, SMTP, FTP, LDAP, DNS, RADIUS, CONNECTION).
2. To remove the sampler, click on Remove Sampler next to the name of the desired sampler.
A confirmation message is displayed.
3. To modify a sampler, click on Modify Sampler next to the name of the desired sampler.
The Modify Connection Samplers menu is displayed.
 - Revise the values in any of the fields. Table 4–11 describes the Connection sampler menu fields. You can also modify the list of hosts under Perform Sampling from the Following Hosts.
 - Click on Modify.
The Define Thresholds menu is displayed.
4. To modify the threshold values or add new threshold values, click on Modify Thresholds next to the name of the desired sampler.
The Define Thresholds menu is displayed. For a description of the fields, see Table 4–12.
5. To create a new threshold, click on Create.
The Create Threshold menu is displayed. For a description of the fields, see Table 4–12.

4.3.11 Managing Thresholds

When you create or modify a sampler, you can also set thresholds.

Table 4–12 describes the Create Threshold and Modify Threshold menu fields.

Table 4–12: Thresholds Menu Fields

Field	Description
Label	Text to be written on the label on a historical report or in the Performance Monitor user interface. This label typically describes the performance of the sampled server when it falls within the specified threshold range, such as Excellent, Poor, or Inaccessible.
Color	Color used on a historical report graph or in the Performance Monitor user interface to represent the threshold. For example, you might choose Green to represent excellent performance and Red to represent poor performance.
Response Time	Time (in milliseconds) for a response received from the server. If this boundary is set, the threshold is considered exceeded if the response time is greater than this value and if no other threshold with a higher response time is exceeded. Note: If the response time boundary is set, it must be the only threshold for this sampler with that specific response time boundary value.

Table 4–12: Thresholds Menu Fields (cont.)

Field	Description
Server Error	If this boundary is set, a threshold is considered exceeded if the polled server reports an error. Note: there can be only one Server Error and only one Server Inaccessible threshold per sampler.
Server Inaccessible	If this boundary is set, a threshold is considered exceeded if the polled server is reported as inaccessible. Note: there can be only one Server Error and only one Server Inaccessible threshold per sampler.
None	If None is chosen, the Performance Monitor and historical report generation tools can still use the threshold to categorize samples into threshold ranges.
System Call	A system call to be executed if a threshold action is triggered. Section 4.3.11.4 describes how to include dynamic information about the sample being processed within the string that you enter for this field.
E-mail Address	E-mail address of the person to be notified if a threshold action occurs. If this threshold action is triggered, a message containing a preformatted statement will be sent. Section 4.3.11.4 describes how to include dynamic information about the sample being processed within the string that you enter for this field.
Subject Line	Subject of the E-mail message sent if a threshold action is triggered. Section 4.3.11.4 describes how to include dynamic information about the sample being processed within the string that you enter for this field.
Action Trigger	Number of consecutive samples that must fall within the threshold range before the threshold action is taken.

From the Define Thresholds menu, the following options are available:

- Create a new threshold (Section 4.3.11.1)
- Modify a threshold (Section 4.3.11.2)
- Remove a threshold (Section 4.3.11.3)

4.3.11.1 Creating a Threshold

After you fill out the initial Create Sampler menu, the Define Thresholds page is displayed, with default values for the following boundaries:

- Server Inaccessible
- Server Error
- Response Time > 0 ms

The Define Thresholds menu also shows any other defined threshold entries.

To create a new threshold, follow these steps:

1. Click on Create next to New Threshold Entry.
The Create Threshold menu is displayed.
2. In the Label field, enter the text to be used as a label on a historical report graph or the Performance Monitor tool.
3. From the color drop-down list, choose a color to be associated with the threshold boundary on the historical report graph or the Performance Monitor tool.
4. In the Threshold boundary section, choose one of the following boundaries:
 - Response time – Enter the boundary time (in milliseconds).
 - Server Error

- Server Inaccessible
5. In the Threshold Action section, choose one of the following actions:
 - None – The Performance Monitor and historical report generation tools can still use the threshold to categorize samples into threshold ranges.
 - System Call – If a threshold action is triggered, the specified system call will be executed on the system where the data collection server is located as the user nsim.
 - E-mail Address – E-mail address of person to notify. If you choose E-mail Address as an action, also enter a subject for the E-mail address in the Subject Line field.
 6. Enter a value for Action Trigger.
 7. Click on Create.

A confirmation message is displayed on the Define Thresholds menu.

4.3.11.2 Modifying a Threshold

When you select Modify Thresholds on the Define Sampling Parameters menu, the Define Threshold menu is displayed. Default values are set for the following boundaries:

- Server Inaccessible
- Server Error
- Response Time > 0 ms

To modify a threshold, follow these steps:

1. Click on Modify next to the threshold to be modified.
The Modify Threshold menu is displayed.
2. Modify any of the values for the Label, Color, Threshold Boundary, Threshold Action, or Action Trigger fields.
3. Click on Modify.
A confirmation message is displayed on the Define Thresholds menu.
You can create additional thresholds or modify existing thresholds.
4. Click on Finished With Thresholds to return to the Define Sampling Parameters menu.

4.3.11.3 Removing a Threshold

To remove a threshold, click on Remove next the threshold item to be removed.

A confirmation message is displayed.

4.3.11.4 Token Substitution in Threshold Action Parameter Strings

If the tokens in Table 4–13 are included in a threshold action System Call string, E-mail Address string, or Subject Line string, the tokens will be replaced with the corresponding substitution values from the table. In the case of System Call and E-mail Address strings, any spaces within the substituted value are converted to underscores ("_") to ensure that the substituted value is treated as a single token by the system shell.

Table 4–13: Threshold Action Substitution Tokens

Token	Substitution Value
@IM_AGENT_NAME@	Host name of the data collection agent that reported the sample.
@IM_RESPONSE_TIME@	Response time of the sample.
@IM_SAMPLER_NAME@	"Name" of the sampler. This is an internal tag that is not relevant to users.
@IM_SAMPLER_TYPE@	Sampler type ("HTTP", for example).
@IM_SAMPLER_DESC@	Sampler description.
@IM_SAMPLER_HOST@	Host being sampled.
@IM_SAMPLER_PORT@	Port being sampled
@IM_SAMPLER_FREQ@	Sampling frequency, in milliseconds.
@IM_BYTE_COUNT@	Byte count of the sample.
@IM_SERVER_INACCESSIBLE@	Whether the server being sampled was inaccessible ("true" or "false" is returned).
@IM_SERVER_ERROR@	Whether the server being sampled returned an error ("true" or "false" is returned).
@IM_SERVER_STATUS@	The status code returned by the server being sampled.
@IM_SERVER_STATUS_MSG@	The status message returned by the server being sampled.
@IM_THRESHOLD_VALUE@	The boundary value of the threshold that was triggered by this sample.
@IM_THRESHOLD_LABEL@	The label of the threshold that was triggered by this sample.
@IM_THRESHOLD_COLOR@	The color of the threshold that was triggered by this sample.
@IM_OLD_THRESHOLD_VALUE@	The boundary value of the previously exceeded threshold.
@IM_OLD_THRESHOLD_LABEL@	The label of the previously exceeded threshold.
@IM_OLD_THRESHOLD_COLOR@	The color of the previously exceeded threshold.

4.4 Managing Sampling Hosts

Data collection agents periodically access Internet services and measure access response time. The agents then report the response times back to the central data collection server.

Data collection agents are installed on systems in a network of computers that uses Internet services. These systems are referred to as sampling hosts. Agents become visible to the Internet Monitor user interface whenever the agent configuration program is run on a desired sampling host and the program registers with the data collection server.

After the agent configuration program runs, you need to download and install the agent software on the machine where the agent will run. See Section 2.4 for details.

Section 3.2 provides guidelines on how to install and deploy data collection agents.

To manage Internet Monitor sampling hosts, choose Manage Sampling Hosts from the Internet Monitor main menu. The Manage Sampling Hosts page shows, in tabular format, every sampling host that has been created and its sampling state

and response state. Sampling hosts are created using the Install Agent Software option (Section 2.4).

From the Manage Sampling Hosts menu, you have the following options:

- Enable or disable sampling hosts using the buttons in the table (Section 4.4.1)
- Remove sampling hosts using the buttons in the table (Section 4.4.2)
- Shut down sampling hosts using the buttons in the table (Section 4.4.3)
- Set a sampling host access password (Section 4.4.4)
- Set access control for sampling host connections (Section 4.4.5)
- Install Agent Software (Section 2.4)

4.4.1 Enabling or Disabling Sampling Hosts

You can either enable or disable data collection agents running on specific sampling hosts in the network. Disabling an agent causes it to cease sampling until the agent is reenabled. To do this, follow these steps:

1. Choose Manage Sampling Hosts from the Internet Monitor menu.
The Manage Sampling Hosts menu is displayed with a table of the current sampling hosts. In the Sampling State column, the current sampling state status of the sampling host is indicated (either enabled or disabled).
2. To disable an agent, click on Disable in the table row.
3. To enable an agent, click on Enable in the table row.

4.4.2 Removing Sampling Hosts

You can remove a sampling host if its response state is indicated as Responding. To do this, follow these steps:

1. Choose Manage Sampling Hosts from the Internet Monitor menu.
The Manage Sampling Hosts menu is displayed with a table of the current sampling hosts. In the Response State column, the current response state status of the sampling host is indicated (either responding or not responding).
2. To remove a sampling host, click on Delete in the table row.

4.4.3 Shutting Down Sampling Hosts

When you shut down a sampling host, you disconnect it from the network and cause the agent to exit. The agent will need to be restarted from the system where it is installed to make it run again.

To shut down an agent, follow these steps:

1. Choose Manage Sampling Hosts from the Internet Monitor menu.
The Manage Sampling Hosts menu is displayed, with a table of the current hosts.
2. To shut down an agent, click on Shut Down in the table row.

4.4.4 Setting a Sampling Host Access Password

You can set a password that will be used by all agents when connecting to the data collection server. To do this, follow these steps:

1. From the Manage Sampling Hosts menu, choose Set Sampling Host Access Password.

The Set Sampling Host Access Password menu is displayed.

2. Enter a password in the Password field.
3. Click on Submit.
4. This step only needs to be done once, not for each agent.

Note that setting the agent password will have no effect on agents currently running. Only when these agents are restarted will they be required to provide the new password. They will need to be reconfigured to do so; the installation program gives instructions on how to do this.

4.4.5 Setting Access Control for Sampling Host Connections

You can permit or deny connections to the data collection server from specific sampling hosts or domains.

To do this, follow these steps:

1. From the Manage Sampling Hosts menu, choose Set Access Control for Sampling Host Connections.

The Set Access Control for Sampling Host Connections menu is displayed. Sampling hosts and domains currently defined and their current access controls are displayed in the Allow Connections From and Deny Connections From lists.

2. To define a new entry, enter the name of the host or domain name in the New Entry field, then click on the Allow Access or Deny Access button.
3. To remove a host or domain from the list of allowed connections, click on its name in the Allow Connections From list, and click on Delete.
4. To remove a host or domain from the list of denied connections, click on its name in the Deny Connections From list, and click on Delete.
5. To submit the changes, click on Submit.

Note

Changing access control entries will not take effect until approximately one minute after the change is submitted.

4.5 Monitoring Performance

When you choose the Detail View or the Summary View option from the Monitor Performance page, you launch the Performance Monitor Java applet in a separate browser window. This applet displays, in graphical form, the performance of Internet services, based on the samplers that you have created.

The Performance Monitor applet requires that your Web browser has the Java Version 1.2 plug-in installed. If this plug-in is not installed, you will be prompted to install it.

The Performance Monitor application requires that your system has the Java Version 1.2 Runtime Environment installed.

From the Monitor Performance menu, you have the following options:

- Detail View (Section 4.5.1)
- Summary View (Section 4.5.2)
- Help on Installing the Performance Monitor Application (Section 2.5)

4.5.1 Detail View

To view a graph of performance detail for a specific sampler, follow these steps:

1. Choose Monitor Performance from the Internet Monitor menu.
2. Click on Detail View.

A Performance Monitor page is displayed in a separate browser window. You will see data only if the sampler is attached to an agent that is currently running. The Performance Monitor displays a graph of the response time and average response time for an agents. Below the graph is a table showing the status, the number of samples received, the throughput in kilobytes per second, and the latest, average, minimum, and maximum response times. All time values are in milliseconds. The latest and average fields of the table may also contain a colored icon. The color of the icon corresponds to the color assigned to the threshold that applies to the response time. This window remains open until you click on Close.

3. To choose another sampler, pull down the Sampler list, and click on another sampler name.

4.5.2 Summary View

To view a summary of all samplers, follow these steps:

1. Select Monitor Performance from the Internet Monitor menu.
2. Click on Summary View.

A new browser window opens, displaying a table for each sampler. Each table shows the status, the number of samples received, the throughput in kilobytes per second, and the latest, average, minimum, and maximum response times. All time values are in milliseconds. The latest and average fields of the table might also contain a colored icon. The color of the icon corresponds to the color assigned to the threshold that applies to the response time. This window remains open until you click on Close.

4.6 Generating a Summary Report

Summary reports provide an instant performance snapshot of all of the Internet services currently being monitored. To generate a summary report, choose Generate Summary Report from the Internet Monitor menu. Table 4–14 describes the information shown in a summary report for each sampler that has been created.

Table 4–14: Summary Report Information

Category	Description
Sampling Target	Description of the sampler.
Last sampled	Timestamp of the most recent sample collected by the sampler.
Response time	Response time of the most recent sample.
Status	The name and color of the threshold range for the most recent sample. If the most recent sample indicated a server error, a link is displayed that will pop up a window with additional error details when clicked upon.
Detailed reports	Links to more detailed historical reports for the last one, six, 12 and 24 hours.

The summary report page is configured to automatically refresh itself with the latest performance information every 10 minutes if it is left in a browser window continuously for longer than that period of time.

Figure 1–7 show a sample summary report.

4.7 Generating Detailed Reports

Historical reports allow administrators to review the past performance of their Internet servers. The administrator can specify:

- Which samplers to report
- List of agents to report for a given sampler
- Period of time to report
- Specific details to be shown on the report

To generate a detailed report, follow these steps:

1. Choose Generate Detailed Reports from the Internet Monitor menu.
The Generate Reports menu is displayed.
2. In the Sampler Description list, click on the name of the sampler to be used for the report.
3. In the Sampling Host list box, click on ALL or on the name of a specific sampling host to be used for the report.
4. Under Display Samples Collected, specify the reporting period by clicking on one or more of the following check boxes:
 - Any Time – If you select this option, the report will include information for all samples collected.
 - Within the range of a specific duration – Pull down the list of options (last hour, current day, previous week, and so on) and choose one of the options.
 - After a specific date and time – Pull down the list of options (month, date, year, hours, and minutes) to specify the times desired.
 - Before a specific date and time – Pull down the list of options (month, date, year, hours, and minutes) to specify the times desired.
5. Under Reporting Options, select the check box next to any of the report details desired. Table 4–15 describes the reporting options.
6. Click on Submit.

Table 4–15: Detailed Report Generation Options

Option Name	Results
Basic sampling statistics	Table of basic statistics such as number of samples processed, low, high, and average response times, byte count, and calculated throughput.
Combined sampling host summary	Section containing combined statistics on multiple sampling hosts. Only effective if ALL is selected from the Sampling Hosts menu and the sampler actually was running on multiple active sampling hosts during the specified reporting period.
Service status distribution table	Statistics on how often the service was accessible, was inaccessible, and reported service errors during the specified reporting period.
Service status distribution graph	Information similar to Service status distribution table but displayed in graphical form.
Threshold distribution table	Statistics on how often service performance fell into each of the defined threshold levels during the specified reporting period.

Table 4–15: Detailed Report Generation Options (cont.)

Option Name	Results
Threshold distribution graph	Information similar to Threshold distribution table but displayed in graphical form.
Service inaccessibility details	Detailed information on each period of service inaccessibility during the specified reporting period.
Service error details	Detailed information on service errors experienced during the specified reporting period.
Sampling period timeline table	Information on how service performance varied with time throughout the duration of the reporting period. This report section is only available for the standard reporting periods in the "Within the:" menu on the Generate Reports menu.
Sampling period timeline graph	Information similar to Sampling period timeline table but displayed in graphical form.

Figure 1–4, Figure 1–5, and Figure 1–6 show a sample detailed report.

4.8 Performing Maintenance Functions

Depending on how many samplers you have set up and how frequently they are set to poll, the sampler database can become quite large. By periodically archiving your database to a backup disk or tape, you can control the file space taken up by the database.

When old samples are written to an archive, they are removed from the samples database, reducing its size and boosting the performance of tools that access it. If desired, the archived records can be merged back into the database at a later time.

Section 3.1 provides more information about sizing the sampler database.

The Internet Monitor provides the following options from the Manage Data menu:

- Set database archiving parameters (Section 4.8.1)
- Enable or disable database archiving (Section 4.8.2)
- Set access control for the Internet Monitor Administration Server (Section 4.8.3)
- Manage Supported Sampler Types (Section 4.8.4)

4.8.1 Setting Database Archiving Parameters

To set archiving parameters, follow these steps:

1. Choose Perform Maintenance Functions from the Internet Monitor menu.
2. On the Perform Maintenance Functions menu, choose Set Archiving Parameters.

The Set Archiving Parameters menu is displayed.

3. In the Archive Directory field, enter the path of the directory to set or modify the archive directory.
4. In the Archive Frequency field, enter the frequency for archiving the database. The archive program is activated daily by the `cron` program. The archive program will process the data only if the number of days specified in this field has elapsed since the time of the last archive.

Note

The `cron` program is executed daily at 1:00 AM, by default.

5. In the Age Requirement field, enter a value to specify how long the archive should be kept in the archive directory. Any data older than the specified number of days will be archived during the next invocation of the archive application. The archive date calculated is relative to midnight of the day the archive program was invoked.
6. Under Archive Retention, use the option button to choose one of the following:
 - All Archives – Retain all archived database files.
 - A specific integer to identify the number of archives to retain. Enter a value in the field.
 - No Archives
7. Click on Submit.

4.8.2 Enabling and Disabling Database Archiving

To enable or disable archiving, follow these steps:

1. Choose Perform Maintenance Functions from the Internet Monitor menu.
2. On the Perform Maintenance Functions menu, choose Enable or Disable Archiving.

The resulting page identifies the current status of archiving: either enabled or disabled.
3. To enable archiving, click on Enable. To disable archiving, click on Disable.

4.8.3 Setting Access Control for the Internet Monitor Administration Server

By default, the `http://host.domain.name:8086/` URL can be accessed only from a Web browser that is running on the same system as the Internet Monitor. If you wish, you can allow access to this URL from Web browsers running on remote systems. You can permit or deny connections to the Internet Monitor Administration Server from specific hosts or domains.

To do this, follow these steps:

1. Choose Perform Maintenance Functions from the Internet Monitor menu.
2. From the Perform Maintenance Functions menu, choose Set Access Control for Internet Monitor Administration Server.

The Set Access Control for Internet Monitor Administration Server menu is displayed. Current access controls are displayed in the Allow Connections or Deny Connections lists.

 - To define a new entry, enter the name of the host or domain name in the New Entry field, then click on Allow Access or Deny Access button.
 - To remove a host or domain from the list of allowed connections, click on its name in the Allow Connections From list, and Click on Delete.
 - To remove a host or domain from the list of denied connections, click on its name in the Deny Connections From list, and Click on Delete.
3. To submit the changes, click on Submit.

If the Administration utility for Internet Express is installed, you can use the Secure Web Server Administration menu to manage access the Internet Monitor Administration Server.

For details about changing access control entries with the Secure Web Server, see the *Secure Web Server Administration Guide*.

4.8.4 Managing Supported Sampler Types

The Manage Supported Sampler Types menu offers these options:

- Add a New Sampler Type (Section 4.8.4.1)
- Change Sampler Type Ordering Section 4.8.4.2)
- Modify or Remove an Existing Sampler Type (Section 4.8.4.3)

4.8.4.1 Adding a New Sampler Type

You can enable the Internet Monitor to monitor network services that are not supported by the default set of samplers.

Before adding a new sampler type, you need to create a Java classes and Java server pages that allow the new service type to be configured and monitored. The new sampler extension framework (Chapter 5) makes this task possible.

Table 4–16 describes the fields in the Create Sampler Type and Modify Sampler Type menus.

Table 4–16: Sampler Type Menu Fields

Option Name	Description
Sampler Type Name	A short string of nonwhitespace characters that uniquely identifies the sampler type. Typically, the protocol being sampled is used (for example, HTTP, FTP, IMAP, and so on).
Report Label	A label used to describe the service monitored by this sampler type. For example, the HTTP service has a report label of “Web servers”. This label is used as the section header for samplers of this type.
Sampler Class	The fully specified name of the Java class that implements the sampling functionality for this sampler type.
Configuration Class	The fully specified name of the Java class that the data collection server can use to store, retrieve, and delete samplers of this type from the configuration database.
UI Bean Class	The fully specified name of the Java class that supports this sampler type’s Management JSP.
Management JSP	The URL of the Java Server Page used to create and modify a sampler of this type. This URL is relative to the Internet Monitor’s Web document root at <code>/usr/internet/monitor/web</code> . Typically, management JSPs for new sampler types are installed in the <code>/usr/internet/monitor/web/config</code> directory ; in this case the URL entered should be something like <code>/config/manage_sampler_mysamplerstype.jsp</code> .
Creation Help URL	The URL of a Web page providing help on the page used to create samplers of this type. The default sampler types specify a section index for the Internet Monitor documentation for this field, but new sampler types should specify an absolute URL or a URL relative to the Internet Monitor’s Web document root at <code>/usr/internet/monitor/web</code> .

Table 4–16: Sampler Type Menu Fields (cont.)

Option Name	Description
Modification Help URL	The URL of a Web page providing help on the page used to modify samplers of this type. The default sampler types specify a section index for the Internet Monitor documentation for this field, but new sampler types should specify an absolute URL or a URL relative to the Internet Monitor's Web document root at <code>/usr/internet/monitor/web</code> . A single Web page is usually sufficient to provide help for both the create and modify processes, in such cases the Modification Help URL and the Creation Help URL can be set to the same value.
Sampler Type Enabled	A check box that specifies whether the information from the sampler type is displayed elsewhere in the Internet Monitor's user interface, including other menus and in reports. By default, the sampler type is enabled.

To add a new sampler type, follow these steps:

1. From the Internet Monitor menu, choose Perform Maintenance Functions.
2. From the Perform Maintenance Functions menu, choose Manage Supported Sampler Types.
The Modify Sampler Type menu is displayed. Current values for each of the sampler type options are displayed.
3. Choose Add a New Sampler Type.
The Add Sampler Type menu is displayed.
4. Enter values for each of the fields on the menu. Table 4–16 describes the fields.
5. If the check box next to Sampler type enabled is checked, the new sampler type will appear elsewhere in the user interface. To prevent the sampler type from being displayed in the user interface, clear the box.
6. To submit the changes, click on Submit.

4.8.4.2 Changing Sampler Type Ordering

You can control the ordering in which sampler types are displayed elsewhere in the user interface. For instance, the Define Sampling Parameters drop-down menu uses this ordering, and the list of current samplers on that page uses it as well. Likewise, the Summary Report page uses this ordering, as does the menu of samplers on the Generate Reports page.

To change the sampler type ordering, follow these steps:

1. From the Internet Monitor menu, choose Perform Maintenance Functions.
2. From the Perform Maintenance Functions menu, choose Manage Supported Sampler Types.
The Modify Sampler Type menu is displayed. Current values for each of the sampler type options are displayed.
3. Choose Change Sampler Type Ordering.
The Change Sampler Type Ordering page is displayed, showing the current order of the sampler types.
4. Move the sampler type up or down in the list:
 - To move a sampler type up in the list, click on its name, then select the Move Selected Type Up button.

- To move a sampler type down in the list, click on its name, then select the Move Selected Type Down button.
5. To submit the changes, click on Submit.

4.8.4.3 Modifying or Removing a Sampler Type

Sampler types can be modified. For example, if you want to specify a different Web page for help on creating or modifying the sampler type, you can enter a URL for that Web page. Sampler types that have been previously added by the administrator can also be removed. The default sampler types that ship with the Internet Monitor cannot be removed, although they can be modified or disabled.

To modify an existing sampler type, follow these steps:

1. From the Internet Monitor menu, choose Perform Maintenance Functions.
2. From the Perform Maintenance Functions menu, choose Manage Supported Sampler Types.
The Manage Sampler Types menu is displayed, indicating all currently recognized sampler types.
3. Select Modify next to the name of the sampler type to be modified.
The Modify Sampler Type menu is displayed. Current values for each of the sampler type options are displayed.
4. Modify any desired values for each in the fields on the menu. Table 4–16 describes the fields.
5. If the check box next to Sampler type enabled is checked, the new sampler type will appear elsewhere in the user interface. To prevent the sampler type from being displayed in the user interface, clear the box.
6. To submit the changes, click on Submit.

If default sampler types that ship with the Internet Monitor are modified, they can be restored to their original values by following these steps:

1. From the Internet Monitor menu, choose Perform Maintenance Functions.
2. From the Perform Maintenance Functions menu, choose Manage Supported Sampler Types.
The Manage Sampler Types menu is displayed, indicating all currently recognized sampler types.
3. Select Modify next to the name of the sampler type to be modified.
The Modify Sampler Type menu is displayed. Current values for each of the sampler type options are displayed.
4. Click the Restore Default Values button.
5. Confirm your choice.

To remove a sampler type, follow these steps:

1. From the Internet Monitor menu, choose Perform Maintenance Functions.
2. From the Perform Maintenance Functions menu, choose Manage Supported Sampler Types.
The Manage Sampler Types menu is displayed, indicating all currently recognized sampler types.
3. Select Remove next to the name of the sampler type to be removed.
4. Confirm your choice.

Using the Sampler Extension Framework

The Internet Monitor Sampler Extension Framework is a set of Java classes that programmers can extend to add support to the Internet Monitor for sampler types that are not part of the default software. For example, a programmer could use the framework to develop a sampler for monitoring WAP services and then integrate this new sampler type into the Internet Monitor software.

5.1 Using the Example Web Sampler

The Internet Monitor ships with example source code that uses the Sampler Extension Framework to implement a simple HTTP sampler called the Web sampler. This is a reduced version of the main HTTP sampler that ships with the Internet Monitor. It is identified in the Web-based user interface as sampler type WEB. The Web sampler example can be built and installed by performing the following steps:

1. Log in to the Internet Monitor host as the `root` user.
2. Run the following commands, in the order shown:

```
# cd /usr/internet/monitor/web/examples/mysamplers
# ./build
# ./install
```
3. Use your Web browser to access the Internet Monitor administration user interface on port 8086 and follow the instructions presented in the installation script on how to register the new sampler type with the Internet Monitor.

Copy the contents of this example directory to a new location and use it as the starting point for any new sampler types you develop. Multiple sampler types can be developed in the same directory and packaged into a single jar file if desired. The example build script does this by default. The jar file produced by the build script will have the same name as the base name of the directory where it is built. For example, if the example is copied to a directory called `/home/smith/newsamplers` and built, a file called `newsamplers.jar` is produced. For consistency, the developer would probably modify the package names of the Java files to be `newsamplers` or something more explicit like `com.company.product.newsamplers`.

5.2 Accessing API Documentation

Writing a new sampler type will require the use of a number of Internet Monitor classes and methods. The example Web sampler demonstrates the use of most of these APIs. You can also find Java documentation for all of the relevant Internet Monitor classes in a gzipped tar file at `/usr/internet/monitor/web/examples/doc.tar.gz` on the host where the Internet Monitor has been installed. Unpack this file and use a Web browser to access the resulting documentation.

5.3 Writing New Sampler Types

The following basic steps required to create a new sampler type are explained in detail in the following sections:

1. Establish the build environment (Section 5.3.1)

2. Create the sampler class (Section 5.3.2)
3. Create the sampler configuration class (Section 5.3.3)
4. Create the sampler user interface bean (Section 5.3.4)
5. Create the sampler management JSP (Section 5.3.5)
6. Build and install the new sampler type (Section 5.3.6)
7. Register the new sampler type with the Internet Monitor (Section 5.3.7)

The following documentation describes the basic process of developing a new sampler type; the example Web sampler source code and comments should be examined for further detail on how to accomplish most of the steps outlined.

5.3.1 Establish the Build Environment

The example build script can be used to build user-defined sampler types on the same machine where the Internet Monitor is installed. To build them on another machine, the `/usr/internet/monitor/web/WEB-INF/lib/imon.jar` file must be copied to the new machine and added to the Java CLASSPATH. It will also be necessary to add the servlet extensions jar file to the CLASSPATH; a copy of the jar file can be found at `/usr/internet/httpd/tomcat/lib/servlet.jar` on the machine where the Internet Monitor is installed.

5.3.2 Create the Sampler Class

The sampler class encompasses the functionality necessary to establish the polling parameters for a specific sampler type, to actually perform the polling operation, and to send the results of a polling operation back to the caller. Instances of this class are typically created by the data collection server for each configured sampler and then passed through RMI to the data collection agents that have been configured to run them. The naming convention for this class is `AbcSampler`, where `Abc` is the name of the protocol being sampled (HTTP, for example). The class must extend `com.compaq.osis.ism.sampler.SamplerImpl` and implement the following functionality:

- Define all protocol-specific instance variables, get methods, and set methods necessary to configure the object for sampling the chosen protocol.
- In the constructor, do the following:
 - Call the superclass constructor.
 - Call superclass methods to override superclass sampler parameters where necessary. Typically, `setPort()` is called to set the default port for the sampled protocol and `setType()` is called to set the sampler type string. The sampler type string is used to uniquely identify this sampler type; it should be a short string of non-whitespace characters. Usually the protocol name (HTTP, NNTP, and so on) is sufficient.
 - Set the `polledDataLabel` instance variable. This string is used during report generation to describe the results returned by the `getPolledData()` method as described in the following.
- Implement a `poll()` method. When a data collection agent is running a sampler, it tracks how often polling is supposed to take place and invokes the sampler's `poll` method at the appropriate times. The `poll` method is responsible for performing a sampling operation using the parameters defined for the sampler, timing the result, and reporting this information to the data collection agent.

Information is reported by initializing a `SamplerEvent` object with the results of the sampling operation and using the superclass `sendEvent()` method to

pass the event to the data collection agent. The `SamplerEvent` class defines methods for setting the response time observed, the number of bytes received, the status code returned by the sampled server, whether the sampled server was inaccessible or returned an error, and any error or status message returned by the sampled server.

- Implement a `getPolledData()` method that returns an array of strings that represent the sampler's polling operations in a format that can be read by a developer. For instance, an HTTP sampler might return a list of the URLs that it is sampling, and the `polledDataLabel` (described previously) might be set to "URLs sampled" to describe this information. Both the polled data and the polled data label are used in historical report generation.
- Implement a `main()` method. This is optional, but useful for debugging the sampler outside the context of a data collection agent. A `DebugSamplerListener` can be created to report received `SamplerEvents` to `stdout`.

5.3.3 Create the Sampler Configuration Class

Sampler configuration information is stored in a JDBC-accessible database. The sampler configuration class is used to save, restore, and delete samplers of a given type to and from this configuration database. The data collection server restores saved samplers from the database at startup; and deletes or saves samplers to the database whenever samplers are created, modified, or deleted through the Web-based configuration user interface.

The sampler configuration class uses the naming convention `AbcSamplerConfig`, where *Abc* is the sampler type name. The class must extend `com.compaq.osis.ism.dcs.SamplerConfig` and provide the following functionality:

- An `initialize()` method that is invoked by the other methods outlined as follows. This method creates any database table needed by the sampler type. This can be accomplished through the `ConfigAccess.initTable()` method, which checks if a given database table exists and creates it if it does not. Once it is known that the database table exists, subsequent calls to `initialize()` can return immediately.

When specifying column data types in the table creation call, do not hardcode data types specific to a particular database product. Instead, use the column type strings defined by the `com.compaq.osis.ism.dcs.DbAccess` class. These column type strings can be overridden in a properties file, allowing the Internet Monitor to run on top of an alternate database by specifying the correct data type property settings for that database. For more information on the data type strings that can be used, see Section 3.7.

- A `restoreConfig()` method that restores the protocol-specific information for the specified sampler from the database. The `restoreConfig()` method must first call `SamplerConfig.restoreConfig()`, so that the superclass can restore the sampler's protocol-independent information. The method must then perform the necessary database calls to retrieve the protocol-specific information for the specified sampler, and then initialize the sampler with the retrieved information. The database can be queried using the superclass `executeQuery()` method to perform an SQL query. The `ResultSet` and associated `Statement` object must be closed afterwards using the `ResultSet.close()` and `ConfigAccess.rsCloseStatement()` methods.
- A `saveConfig()` method that saves the protocol-specific information for the specified sampler to the database. The `saveConfig()` method must first call `SamplerConfig.saveConfig()`, so that the superclass can save the protocol-independent sampler information. After that, the protocol-specific

sampler information can be saved using the superclass `executeUpdate()` method to perform an SQL insertion.

- A `deleteConfig()` method that deletes the protocol-specific information for the specified sampler from the database. This can be accomplished using the superclass `executeUpdate()` method to perform an SQL deletion. After doing this, the method must call the superclass `deleteConfig()` method, so that the superclass can delete the protocol-independent sampler information for the specified sampler.

5.3.4 Create the Sampler User Interface Bean

The sampler user interface bean serves as an interface between the sampler management JSP and the data collection server. Together, they allow a new sampler type to be integrated into the Internet Monitor Web-based administration user interface so that administrators can create, modify, and perform other operations on samplers of this type. The user interface bean should be designed to have properties that match the form field names in the JSP used to create and modify samplers of that type.

The sampler user interface bean uses the naming convention `AbcSamplerUIBean` where `Abc` is the sampler type name. It must extend `com.compaq.osis.ism.config.SamplerUIBean` and implement the following functionality:

- The bean constructor must call the `superclass()` constructor and then initialize the bean properties to default values. This can include initializing properties defined in the bean as well as overriding the defaults for superclass properties. The default values set here will be used to initialize form fields in the JSP-generated sampler creation page. For text-based form fields that should be empty by default, use the empty string (`""`) as a default value.
- For each of the protocol-specific form fields in the sampler management JSP, create a set method with the same case-adjusted name as the form field (for example, a text input field named “path” in the JSP should have a corresponding method called `setPath()` in the bean). This method will be called when the JSP is processed, it should be used to store the information from the JSP form fields in instance variables for later processing.
- For each of the protocol-specific form fields in the sampler management JSP, implement a get method that returns a value used to initialize that form field. This get method should do one of two things:
 - If the superclass `currentSampler` instance variable is null, a sampler creation is taking place, and the method should return the default property value.
 - If the `currentSampler` value is set, a sampler modification is taking place, and the method should retrieve the appropriate information from the `currentSampler` and return it. The JSP will then use the returned information to initialize its corresponding form field.
- The bean should implement a `processRequest()` method, which will be called by the JSP after the bean properties have been initialized. This method should call the `validateProperties()` method, create a new uninitialized sampler of the appropriate type, call the `configureSampler()` method with this sampler as a parameter, and finally call the `commitOperation()` method. The routine should catch any `UIBeanExceptions` or `Exceptions` thrown by any of these methods. If exceptions are caught, a `ConfigResult` object with a `ConfigResult.FAILURE` type and a message extracted from the exception should be returned. Otherwise, a `ConfigResult` object with a `ConfigResult.SUCCESS` type should be returned.

- Implement a `validateProperties()` method. This method should first call the superclass version, and then validate the data in all protocol-specific properties. If any data is invalid (number out of range, blank string where a value is required, and so on), a `UIBean` exception should be thrown. This will be caught by `processRequest()`, which will return a `ConfigResult` failure to the JSP. Note that much of this property validation can instead be done using JavaScript in the sampler management JSP. The `validateProperties()` method handles any cases that are not or cannot be validated using JavaScript within the management JSP.
- Implement a `configureSampler()` method. This method should invoke the superclass version, and then apply the data from the protocol-specific properties to the specified sampler.
- Implement a `commitOperation()` method. Normally, this method does nothing more than call the superclass version. This method communicates the configuration changes to the data collection server, which stores them in the configuration database.

5.3.5 Create the Sampler Management JSP

A sampler management JSP is invoked from the Web-based management user interface, whenever the administrator attempts to create or modify a sampler of a particular type. The sampler management JSP is combined with other JSP files that implement the user interface for fields that are common to all sampler types and a resulting sampler creation or modification HTML page is generated.

The sampler management JSP uses a naming convention of `manage_sampler_abc.jsp`, where `abc` is the sampler type name in lower case. It should contain the following sections:

- A JSP page import statement that specifies the class for the corresponding sampler user interface bean.
- A JSP `useBean` tag creates a bean with an ID of `cfgbean`, a request scope, and a class equal to the corresponding sampler user interface bean.
- A JavaScript section containing a function called `checkSamplerFields()`. This function is invoked when the user clicks on the Submit button, it should be used to validate the form input from the protocol-specific portions of the page, raising an alert and returning false if there is a problem and returning true otherwise.
- A section of HTML code that defines the user interface for configuring the protocol-specific portions of the sampler. The values used to initialize the form fields can be obtained by calling the corresponding get methods in the sampler user interface bean. These methods will return proper default values in the case of a sampler creation and proper values from the sampler being modified in the case of a modification.

5.3.6 Build and Install the New Sampler Type

The class files mentioned previously should be compiled and then combined into a single jar file. The example Web sampler build file (Section 5.3) shows how to do this.

Once built, the example Web sampler install script demonstrates how to install the sampler type. The basic steps the script takes are:

- Stops the Internet Monitor
- Copies the jar file with the new classes to the `/usr/internet/monitor/web/WEB-INF/lib` directory

- Copies the management JSP to the `/usr/internet/monitor/web/config` directory
- Sets the proper file permissions on the copied files
- Restarts the Internet Monitor

5.3.7 Register the New Sampler Type with the Internet Monitor

The final step is to configure the Internet Monitor to know about the new sampler type.

1. Use a Web browser to connect to the Internet Monitor administration user interface on port 8086.
2. From the Perform Maintenance Functions page, select Manage Sampler Types, then select Add a New Sampler Type.
3. Fill in the listed fields as appropriate for the new sampler type. For the example Web sampler type, the values would look like the following:

```

Sampler Type Name : WEB
Sampler Class     : mysamplers.WebSampler
Configuration Class: mysamplers.WebSamplerConfig
UI Bean Class    : mysamplers.WebSamplerUIBean
Management JSP   : /config/manage_sampler_web.jsp

```

4. Click the Help link on the page for more information on the form fields.

After submitting the page, the new sampler type should be operational. Verify that the new sampler type appears as one of the available types in the sampler creation menu, using these steps:

1. Create a sampler of the new type, then modify it.
2. Restart the Internet Monitor to make sure that the sampler was restored properly from the database.
3. Attach the sampler to a sampling host and use the live monitor and historical reporting options to ensure that sampling data is being received from the new sampler as expected.

A

Administration server

setting access control, 4–35

agent

(*See* data collection agent)

alternate database

configuring the Internet Monitor to use,
3–11

archiving

managing, 4–34

C

connection sampler

attaching to a sampling host, 4–25

creating, 4–25

guidelines for deploying, 3–8

managing, 4–24

menu fields, 4–24t

modifying, 4–26

removing, 4–26

D

data collection agent, 1–2

configuring for automatic restart, 2–4

definition, 1–2

determining installation location, 3–1

determining number to deploy, 3–2

downloading software, 2–2

function, 1–2

guidelines for deploying, 3–1

information passed to the server, 1–3

installing software, 2–2

managing, 4–29

recommended installation location, 3–2

data collection server, 1–4

definition, 1–2, 1–4

function, 1–4

database

archiving, 4–34

disabling archiving, 4–35

enabling archiving, 4–35

guidelines for deploying, 3–1

location, 2–2

managing, 4–34

deployment guidelines, 3–1

DNS sampler

attaching to a sampling host, 4–21

creating, 4–20

menu fields, 4–20t

modifying, 4–21

removing, 4–21

domain

setting access control, 4–31

E

E-mail

configuring for target user, 3–5

filtering incoming with procmail

command, 3–6

filtering incoming with slocal command,
3–6

F

firewall environment

configuring Internet Monitor for use
in, 3–9

FTP sampler

attaching to a sampling host, 4–16

creating, 4–16

guidelines for deploying, 3–7

managing, 4–15

menu fields, 4–15t

modifying, 4–17

removing, 4–17

H

historical report

generating, 4–33

HTTP sampler

attaching to a sampling host, 4–5

creating, 4–4

deciding which URIs to access, 3–3

function, 4–3

guidelines for deploying, 3–3

managing, 4–3

menu fields, 4–4t

modifying, 4–6

removing, 4–6

I

IMAP mail server

monitoring, 4–11

IMAP sampler

- attaching to a sampling host, 4–12
- creating, 4–11
- creating target users, 3–4
- guidelines for deploying, 3–4
- managing, 4–11
- menu fields, 4–11t
- modifying, 4–12
- removing, 4–12

installation

- choosing an interface, 2–1
- prerequisites, 2–1

Internet Monitor

- accessing with Administration utility, 4–1
- accessing with Web browser, 4–1
- checklist for getting started, 1–9
- components, 1–1
- configuring to use alternate databases, 3–11
- introduction, 1–1
- main menu, 4–1
- properties file, 3–13
- security guidelines, 3–9
- starting, 4–1
- stopping, 4–1

Internet Service Provider, 1–1

Internet services

- monitoring performance, 4–31
- viewing performance detail, 4–32
- viewing performance summary, 4–32

ISP

(See Internet Service Provider)

J

Java Message Service

(See JMS)

JDBC driver

- installing, 3–13

JMS

- accessing class files, 3–20
- contents of sample message, 3–16
- message body, 3–17
- sample client, 3–20
- specifying configuration using Internet Monitor, 3–20

L

LDAP sampler

- attaching to a sampling host, 4–19
- creating, 4–18
- managing, 4–17
- menu fields, 4–18t
- modifying, 4–19
- removing, 4–19

M

monitor sampler graph

- example, 1–4

N

news server

- monitoring, 4–6

newsgroup, 3–3

(See also target newsgroup)

- creating, 3–3
- limiting export, 3–4
- modifying article expiration definition, 3–4
- posting sample messages, 3–4

NNTP sampler

- attaching to a sampling host, 4–7
- creating, 4–7
- guidelines for deploying, 3–3
- managing, 4–6
- menu fields, 4–6t
- modifying, 4–8
- prerequisites, 3–3
- removing, 4–8

P

Performance Monitor applet

- using in a cluster environment, 3–21

Performance Monitor application,

- 4–31
- downloading, 2–3
- installing, 2–3
- introduction, 1–4
- running, 1–4

POP mail server

- monitoring, 4–8

POP sampler

- attaching to a sampling host, 4–10
- creating, 4–9
- creating target users, 3–4
- guidelines for deploying, 3–4
- limited to one agent, 3–4
- managing, 4–8
- menu fields, 4–9t
- modifying, 4–10
- removing, 4–10

Port field

- function, 4–3

port numbers

- default values, 4–3

PostgreSQL database

- default values, 3–15t

proxy server

- monitoring, 4–3

R

RADIUS sampler

- attaching to a sampling host, 4-23
- creating, 4-23
- guidelines for deploying, 3-7
- managing, 4-22
- menu fields, 4-22t
- modifying, 4-24
- removing, 4-24

Remote Authentication Dial In User Service

(See RADIUS sampler)

report

- generating, 4-33
- generating a summary, 4-32
- introduction, 1-6

S

sampler

- definition, 1-2, 4-2
- determining data to be retrieved, 3-3
- guidelines for configuring, 3-2
- information reported, 1-6
- managing, 4-2
- monitoring performance, 4-31
- overview, 1-2

sampler database

- guidelines for sizing, 3-1
- managing, 4-34

sampler types

- adding, 4-36
- changing the order, 4-37
- managing, 4-36
- modifying, 4-38
- removing, 4-38

SampleReceived message, 3-16

sampling host

- disabling, 4-30
- enabling, 4-30
- managing, 4-29
- removing, 4-30
- setting access control, 4-31
- setting access password, 4-30
- shutting down, 4-30

sampling interval

- choosing, 3-3

sampling parameters

- defining, 4-2

security

- guidelines, 3-9

service level agreements, 1-1

SMTP sampler

- attaching to a sampling host, 4-14
- automatic disposal of new messages, 3-5
- creating, 4-13
- creating target users, 3-4
- guidelines for deploying, 3-7
- managing, 4-13
- menu fields, 4-13t
- modifying, 4-14
- removing, 4-14

T

target newsgroup

- creating with INND news server, 3-3

target user

- creating a user account, 3-5
- creating for IMAP samplers, 3-4
- creating for POP samplers, 3-4
- creating for SMTP samplers, 3-4
- improving security, 3-7
- populating with test messages, 3-5

threshold

- creating, 4-27
- default, 3-8t
- managing, 4-26
- modifying, 4-28
- removing, 4-28
- setting response time, 3-8
- specifying action trigger, 3-8
- specifying multiple tasks, 3-9
- specifying system call action, 3-9
- token substitution, 4-28

threshold action

- guidelines for deploying, 3-8

ThresholdChanged message, 3-18

token substitution, 4-28

U

Uniform Resource Identifier

(See URI)

URI

- specifying in HTTP samplers, 4-3

W

Web server

- monitoring, 4-3